

# Cyber Security Defense

**Know thyself,  
know thy enemy,  
fear not 100  
battles**





# Joseph Muniz

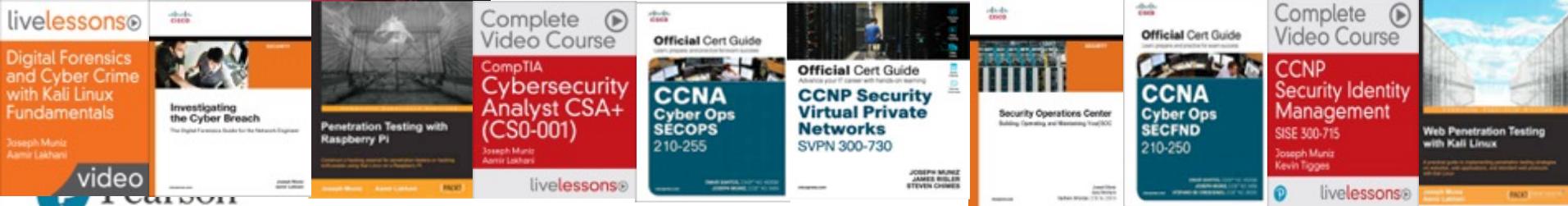
Security Architect – Americas Sales Organization

Security Researcher – [www.thesecurityblogger.com](http://www.thesecurityblogger.com)

Speaker: Cisco Live / DEFCON / RSA / (ISC)2

Avid Futbal Player and Musician

Twitter @SecureBlogger

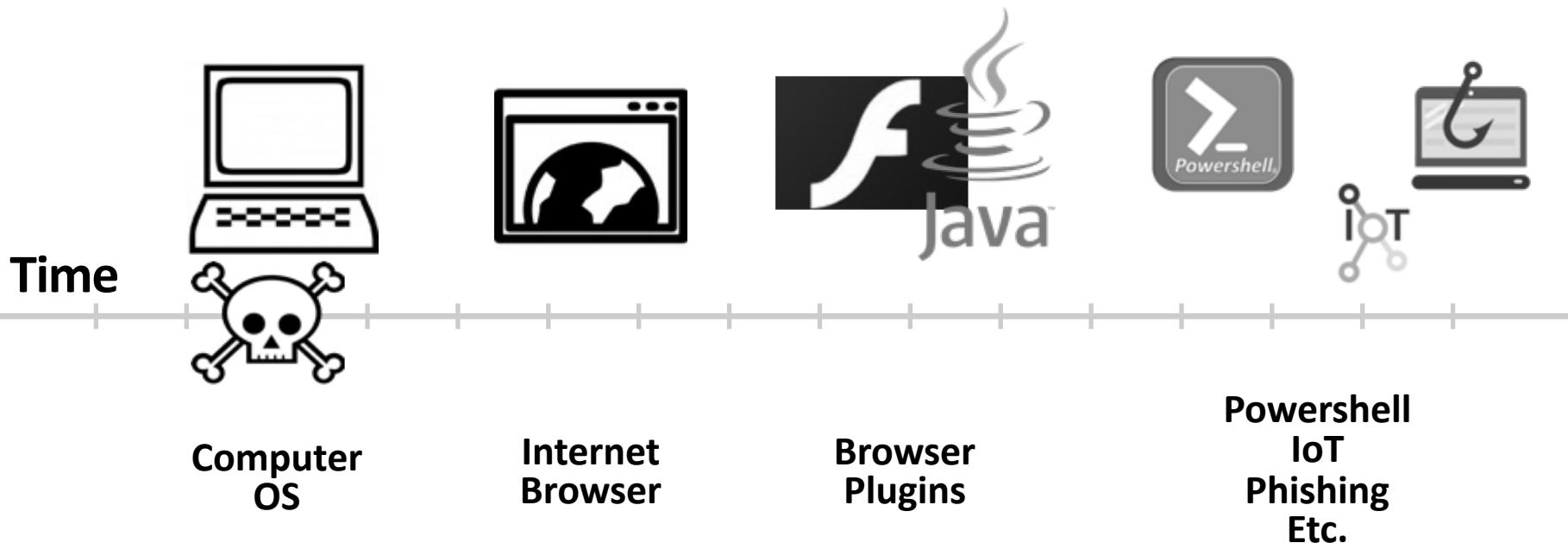


The image shows a row of nine book covers from the livelessons series, all featuring Joseph Muniz as the author. The books are:

- Digital Forensics and Cyber Crime with Kali Linux Fundamentals
- Investigating the Cyber Breach
- Penetration Testing with Raspberry Pi
- Complete Video Course: CompTIA Cybersecurity Analyst CSA+ (CS0-001)
- Official Cert Guide: CCNA Cyber Ops SECOPS 210-255
- Official Cert Guide: CCNP Security Virtual Private Networks SVPN 300-730
- Security Operations Center: Building, Operating and Monitoring Your SOC
- Official Cert Guide: CCNA Cyber Ops SECFND 210-250
- Complete Video Course: CCNP Security Identity Management SISE 300-715
- Web Penetration Testing with Kali Linux



# Cat And Mouse Game



# Adversaries Buy Products Too



# Can't Answer: What Happened?????



# Can't Answer: What Happened?????



Vulnerabilities



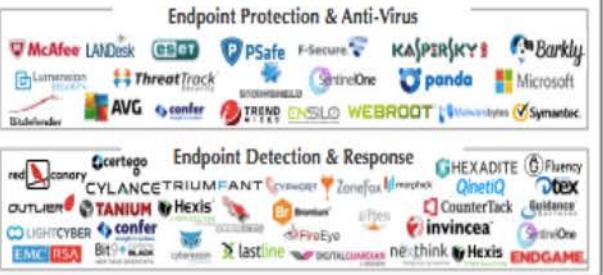
Malicious Sources



## Infrastructure Security



## Endpoint Security



## Application Security



## Security Operations & Incident Response

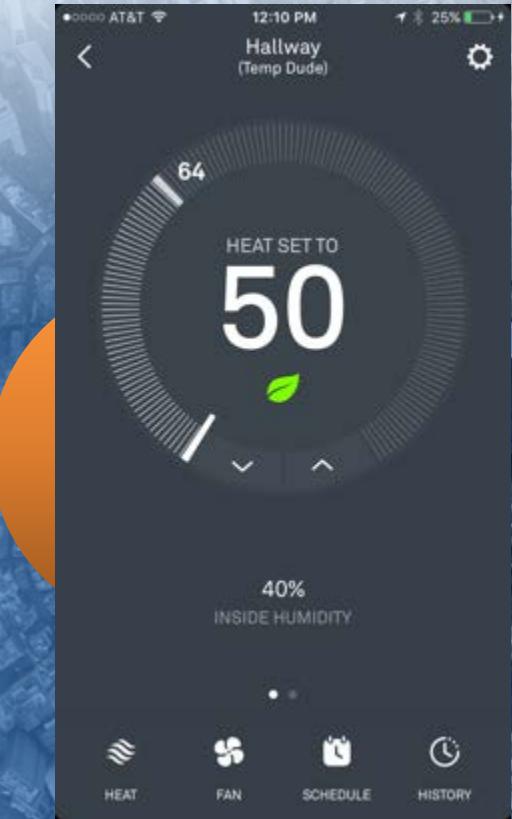


## Risk & Compliance



# But wait ... there's more

# Growth of Internet Connected Devices Continues ...



# IoT Challenges

- Micro drive or plug to access hardware
- Firmware security analysis and modification
- Radio- / wireless-based exploitation
- Application exploitation
- Hardware exploitation (example JTAG)



Patch Delays

Limited Security Development



# Half of US companies hit by IoT security breaches, says survey

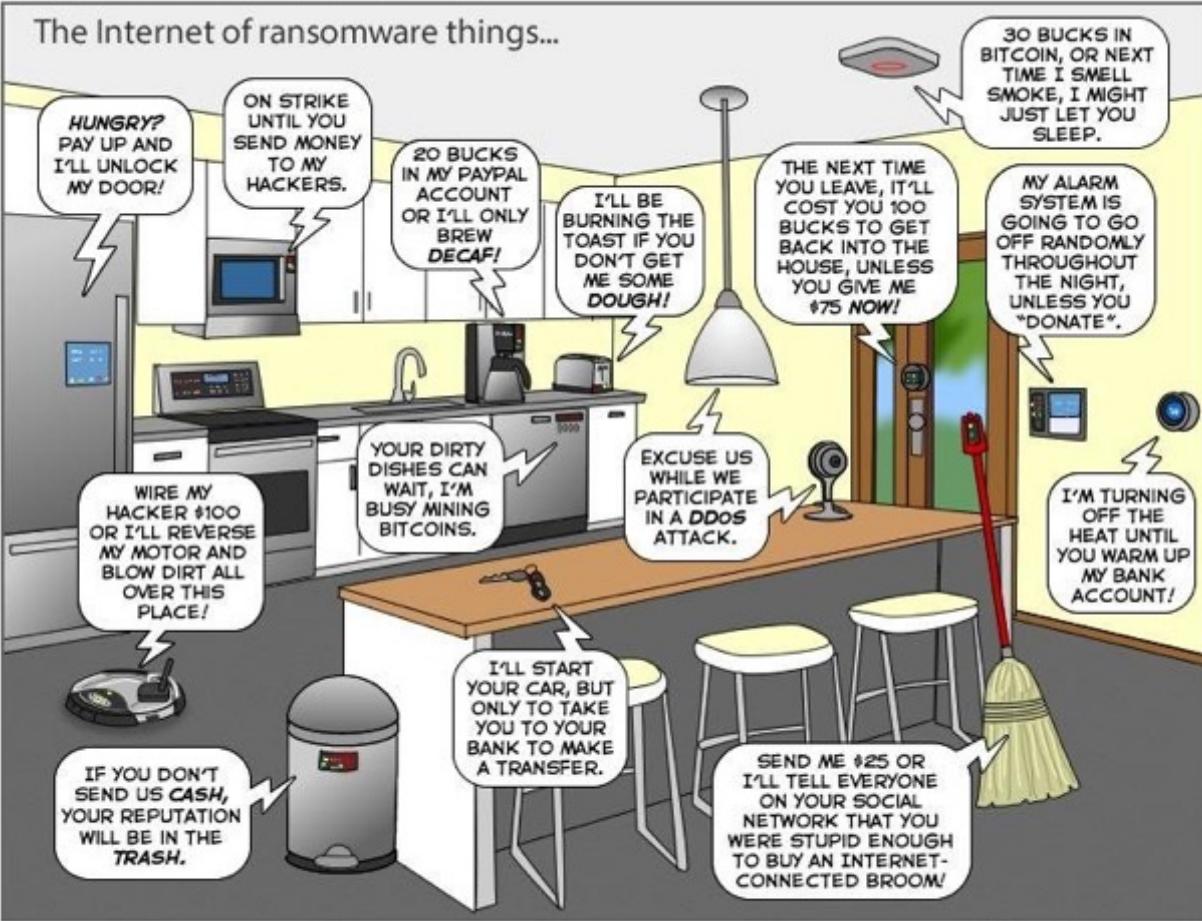
By Freddie Roberts - June 5, 2017

“Want to browse the internet? Pay the ransom. Want to use your baby monitor? Pay the ransom. Want to watch your smart TV? Pay the ransom.”

NEWS

# Half a bread

By Freddie Ro



You can help us keep the comics coming by becoming a patron!  
[www.patreon/joyoftech](http://www.patreon/joyoftech)

[joyoftech.com](http://joyoftech.com)

©2018 Pearson, Inc.

# Lack of Legal Enforcement

**California just became the first state with an Internet of Things cybersecurity law**

By Adi Robertson | @thedextriarchy | Sep 28, 2018, 6:07pm EDT

f t  SHARE

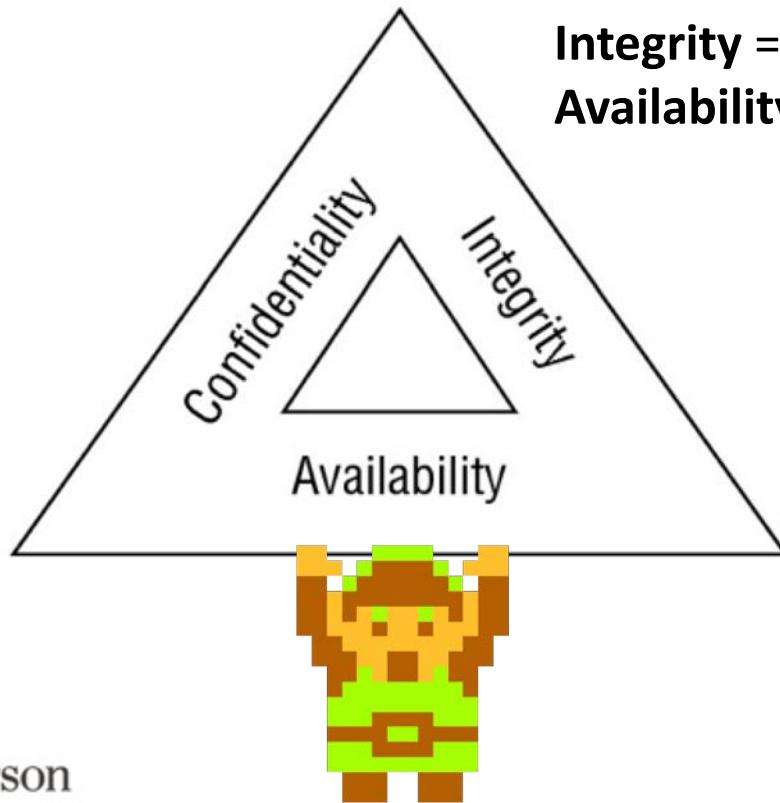


# Agenda

- Risk Management
- Security Operations (SOC)
- Cyber Defense
- Edge Defense
- Host Defense
- Access Control and Segmentation
- Breach Detection and Continuous Monitoring
- Architecture Best Practices
- Training and Certification



# Cybersecurity Goals



# Threats

**Adversarial** – Individual, groups or organizations (Hackers, Anonymous, etc.)



**Accidental** – Mistake that undermines security (configuration error)

**Structural** – Equipment, software or the environment fail (system crashes)

**Environmental** – Natural or man-made disaster (Godzilla / Hurricane)



fact



# Risk 10

**threat** to a

Threat x Vuln

xpectancy x Asset

Single loss expectan



Takes advantage of



To deliver

Objective

# Vulnerabilities

- Weakness in system
- Configuration error, missing patch, flaw in design, etc.
- Signature security defend attacks (exploiting) against vulnerabilities. *Examples IPS, Anti-Virus*

# Malware



Meltdown



Spectre

# Common Vulnerabilities and Exposures (CVE)

Vulnerability Type: Apache vulnerability

Threat Description: Three vulnerabilities in the Apache Struts 2 package

Existing Controls: Firewalled and monitored by IPS

Probability: Unlikely (not web facing)

Impact: Critical

<http://cve.mitre.org/about/faqs.html>

Multiple Vulnerabilities in Apache Struts 2 Affecting Cisco Pr  
2017



<b>Advisory ID:</b>	cisco-sa-20170907-struts2	CVE-2017-9793	Download CVRF
<b>First Published:</b>	2017 September 7 21:00 GMT	CVE-2017-9804	Download PDF
<b>Last Updated:</b>	2017 September 12 19:53 GMT	CVE-2017-9805	Email
<b>Version 1.3:</b>	Interim	CWE-20	
<b>Workarounds:</b>	No workarounds available	CWE-399	

# Joey's Shoes 2.0



# Joey's Shoes 2.0



# Common Vulnerability Scoring System

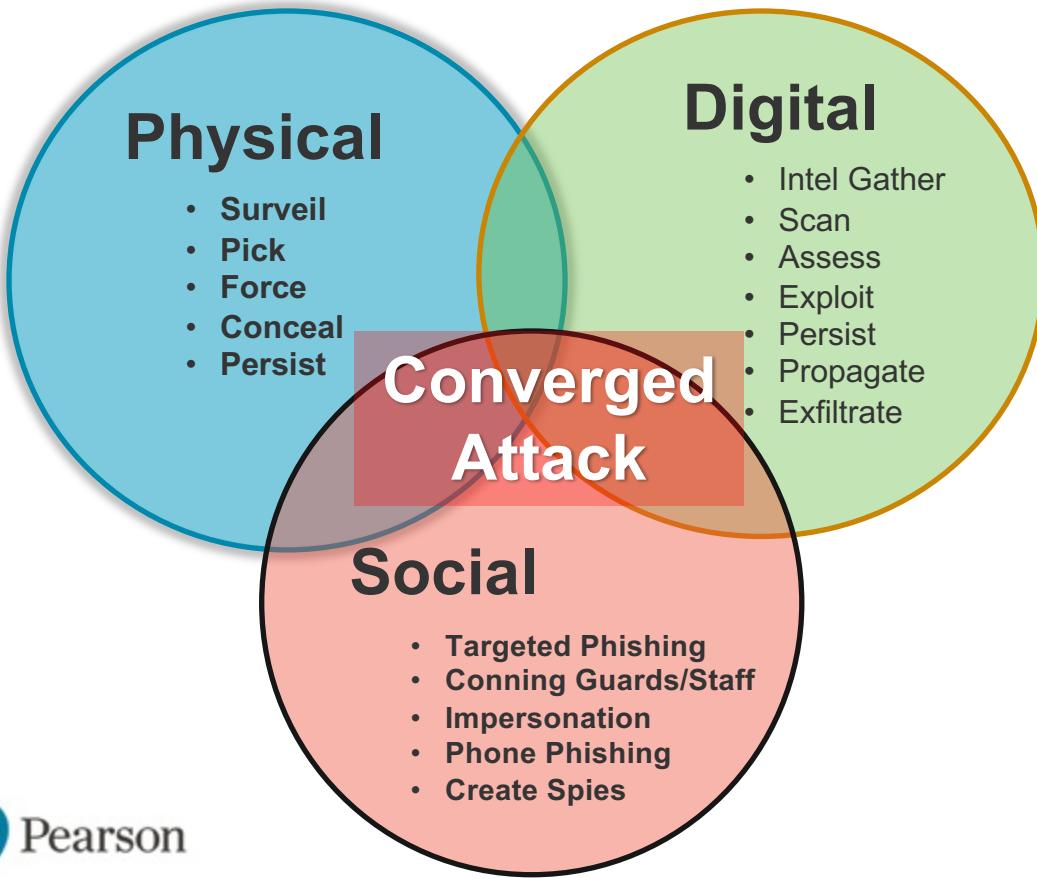
Consistent standard for computing vulnerability severity  
Examples are version 2 and most used but version 3.1 is the latest

Access Vector	Local (L) = 0.395	Adjacent Network (AN) = 0.646	Network (N) = 1.0
Access Complexity	High (H) = .035	Medium (M) = 0.61	Low (L) = 0.71
Authentication	Multiple (M) = 0.45	Single (S) = 0.560	None (N) = 0.704
Confidentiality	None (N) = 0.00	Partial (P) = 0.275	Complete (C) = 0.66
Integrity	None (N) = 0.0	Partial (P) = 0.275	Complete (C) = 0.660
Availability	None (N) = 0.0	Partial (P) = 0.275	Complete (C) = 0.660

# Patching

- Piece of software designed to update a computer program or data to fix or improve it.
- **This includes fixing security vulnerabilities!**
- Sometime could introduce new problems so backup planning should be performed before installing

# Vectors of an Attack



# Physical Attacks

## Keyboard Drivers



## System Backdoor



## Network Backdoor



# Digital Attacks

NMAP shows Open Ports!

Nexpose shows vulnerabilities

Metasploit delivers attack





192.168.1.1:3000/ui/panel

Activat

Disable

Show

## NOTIFICATIONS

On  
Off

On  
Off

 endorsed you for a skill: Cisco Technologies

1h

 endorsed you for a skill: CCNA

1h

- ▶ Get Registry Keys
- ▶ Detect CUPS
- ▶ Get Clipboard
- ▶ Make Telephone Call
- ▶ IPEC (6)
- ▶ Metasploit (0)
- ▶ Misc (4)
- ▶ Network (7)

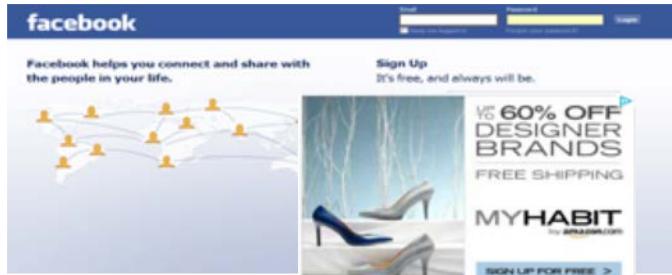
# Example Exploit Kits And Ransomware



User Goes To Website

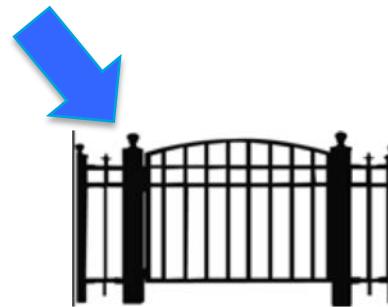


# Example Exploit Kits And Ransomware



Compromised  
Advertisement  
Sends To Gate

User Goes To Website



# Example Exploit Kits And Ransomware



User Goes To Website



Compromised  
Advertisement  
Sends To Gate

Vetted Users Sent To Landing  
Page (could be angler)



# Example Exploit Kits And Ransomware



User Goes To Website



Compromised  
Advertisement  
Sends To Gate

Vetted Users Sent To Landing  
Page (could be angler)

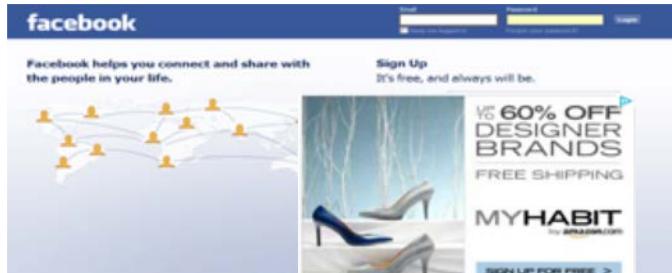


Exploit (maybe Java)



Exploit (maybe Flash)

# Example Exploit Kits And Ransomware



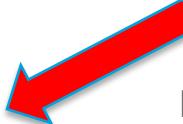
Compromised  
Advertisement  
Sends To Gate

User Goes To Website



Payload Delivered (probably  
Ransomware)

Vetted Users Sent To Landing  
Page (could be angler)



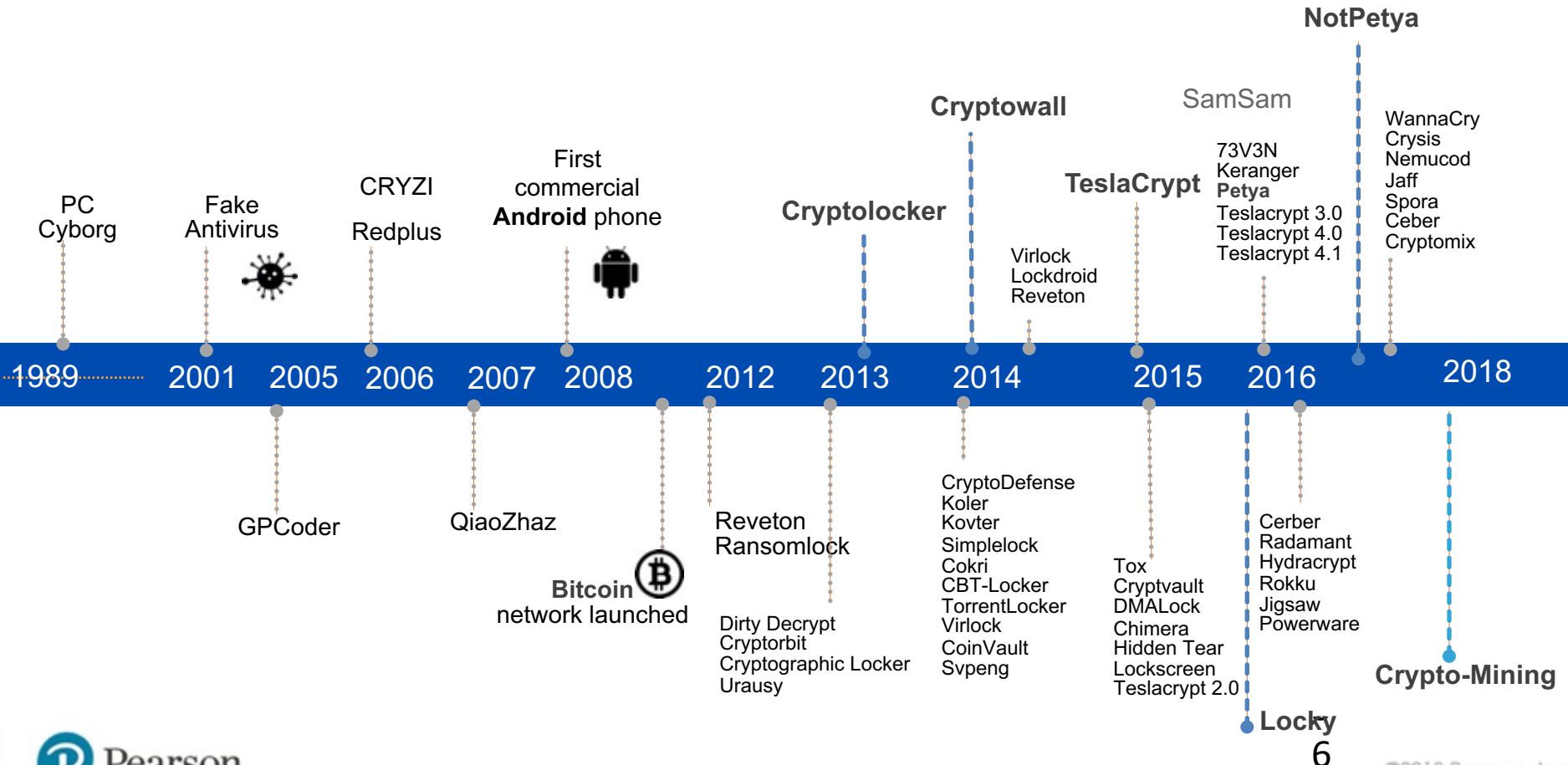
Exploit (maybe Java)



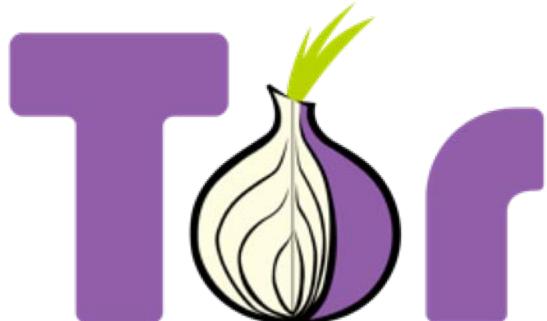
Exploit (maybe Flash)



# The Evolution of Ransomware Variants



# Ransomware Evolution



*bitcoin*

A screenshot of a web page showing a comment section for a ransomware attack. The "Your comments" section contains a message from a user named "black\_gmail" asking for decryption software. The "Our Answer" section contains a reply from the attackers providing a download link for the decryption tool.

Your comments

Leave a comment here with your "Computer name" to receive decryption software.

22/01/2018 18:40 black\_gmail@gmail.com

For All Affected PCs:

Sorry for delay, here you are: [http://e000e000e000e000.myupload.com/index.php?file\\_id=5001994132](http://e000e000e000e000.myupload.com/index.php?file_id=5001994132)

Our Answer

Not decryption for [REDACTED] PC. Check help: [http://e000e000e000e000.myupload.com/index.php?file\\_id=7230120481](http://e000e000e000e000.myupload.com/index.php?file_id=7230120481)

Sorry for delay, here you are: [http://e000e000e000e000.myupload.com/index.php?file\\_id=5001994132](http://e000e000e000e000.myupload.com/index.php?file_id=5001994132)

Leave a comment

Your Email: \_\_\_\_\_

Submit Comment

# Social Engineering + Phishing Themes

## COVID-19: Hackers Begin Exploiting Zoom's Overnight Success to Spread Malware

March 30, 2020 by Ravie Lakshmanan



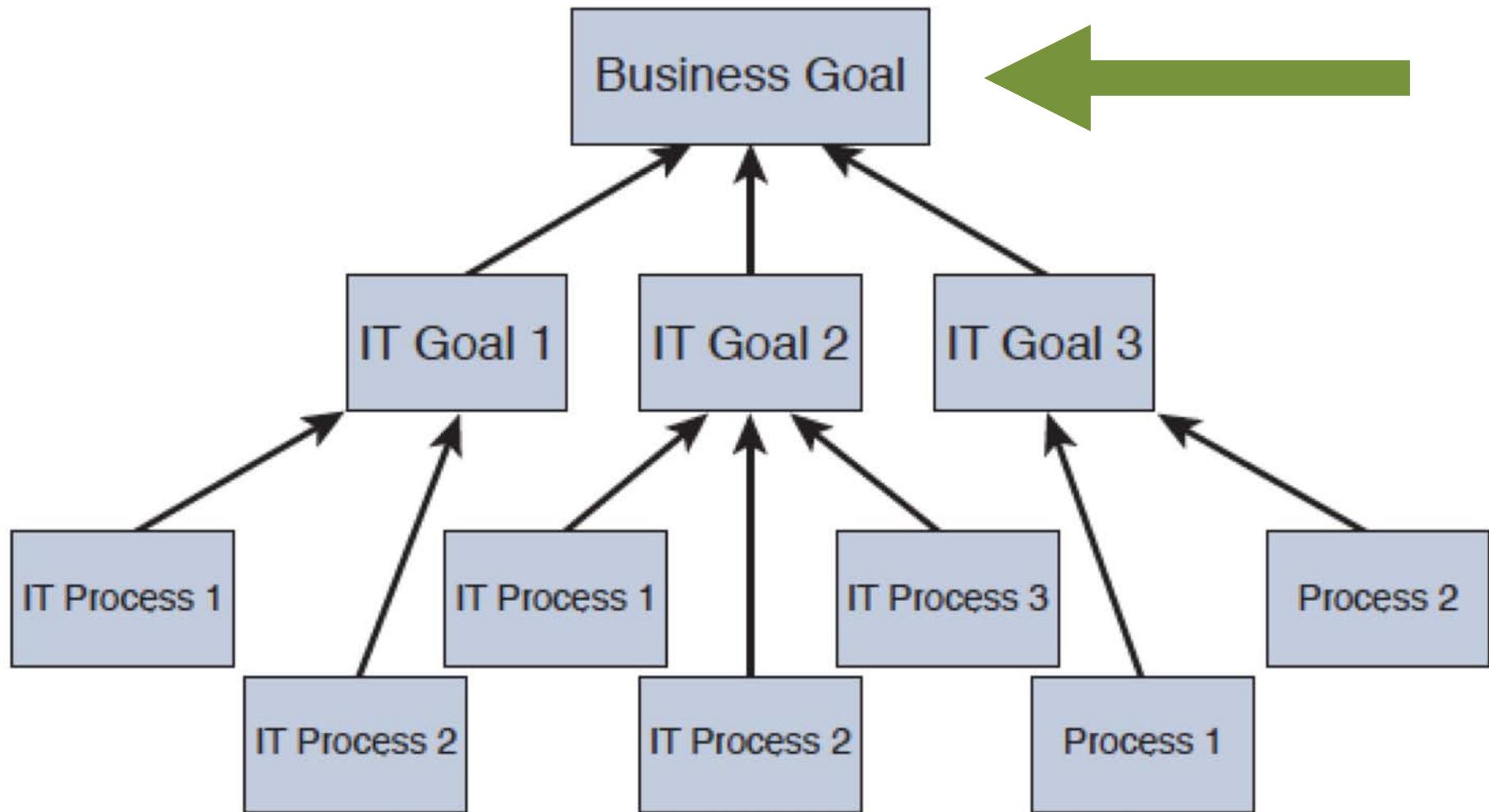
**IN THE HEADLINES**  
TALOS

The ongoing COVID-19 pandemic continues to yield new subject matter that bad actors can turn into fodder for enticing victims into clicking on malicious links and attachments. On March 27, the CARES Act was signed into law by the President, enacting a wide range of stimulus packages designed to aid Americans and businesses during the crisis. One such measure will authorize a supplemental stimulus check to American citizens.



# Security Operations 101





# Need Executive Sponsorship for Success

- Who influences funding?
- What is considered success?
- How is grading achieved?

**Business focus is critical!**





**Single loss expectancy x  
Asset value = Exposure  
factor**

## Prevent Asset Loss

Vulnerability Management

Incident Response

Continuous Monitoring

Information Assurance

Remediation

Forensics

Security Tools

Compliance

HR / Marketing

Risk Management

# ISACA COBIT Maturity Levels

**0 – No Program**

No Capabilities or Processes

**1 – Ad Hoc**

Recognized problems. Ad hoc Approach

**2 – Repeatable  
but intuitive**

Some process but no formal training or procedures. Self ran

**3 - Defined  
Process**

Documented process but up to individual to follow

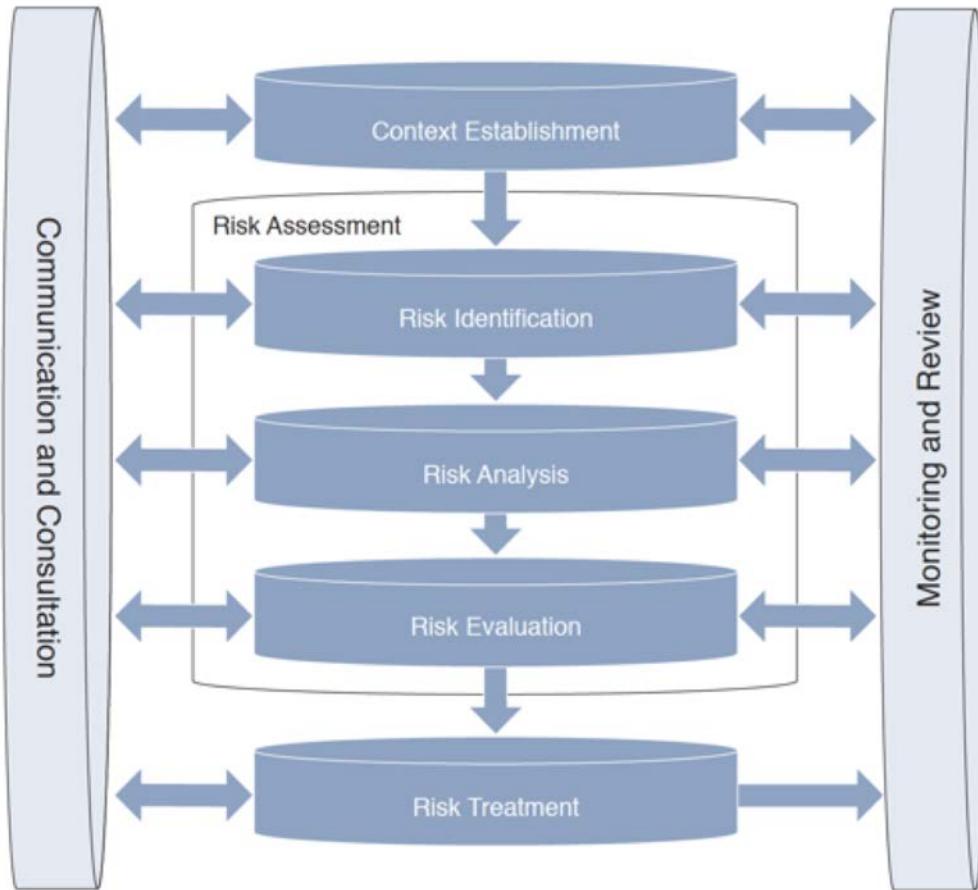
**4. – Managed  
and Measurable**

Monitor and manage compliance. Action can be taken to improve

# SOC Capabilities

- **Risk Management** – Dealing with all Risk
- **Vulnerability Management** – Dealing with specific vulnerabilities
- **Compliance** – Meeting requirements
- **Analysis** – Analyze various types of artifacts
- **Incident Management** – Responding to cyber attacks
- **Digital Forensics** – Understanding what happened
- **Situational and Security Awareness** – Threat awareness
- **Research and Development** – Response to changing landscape

# Service 1: Risk Management



**Formal programs include**

- ISO/IEC 27005:2010
- ISO/IEC 31000:2009
- NIST SP 800-39
- OWASP Risk Rating Methodology
- DoD Risk Management Framework (RMF).

# Risk Actions

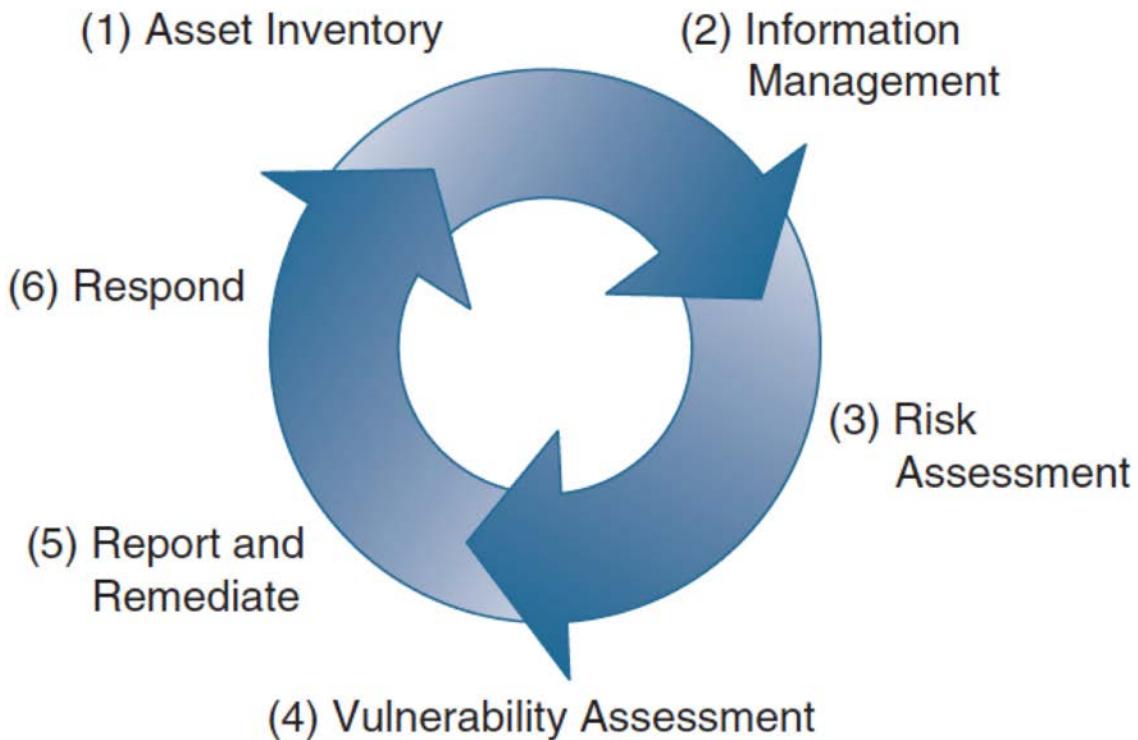
- **Risk Reduction** – Implement Countermeasure
- **Risk Transfer** – Purchase Insurance
- **Risk Acceptance** – Accept a Possible Loss
- **Risk Rejection** – Pretend There Isn't a Risk

# How to prioritize risk

Threat Agent Factors				Vulnerability Factors			
Skill Level	Motive	Opportunity	Size	Ease of Discovery	Ease of Exploit	Awareness	Intrusion Detection
1	7	5	2	6	3	2	9
Likelihood of Threat = 4.375 MEDIUM							

Technical Impact				Business Impact			
Loss of Confidentiality	Loss of Integrity	Loss of Availability	Loss of Accountability	Financial Damage	Reputation Damage	Non-Compliance	Privacy Violation
8	9	7	5	2	2	1	5
Technical Impact = 7.25 EXTREME				Business Impact = 2.25 LOW			

# Service 2: Vulnerability Management



- SANs Example
- NAC and Profiling can help with Asset Inventory
- Triggers
  - CVE Identifier may trigger event
  - Assessment tools
  - Audits

# Service 3: Compliance

- Legal or Business
  - Should be minimal security
  - SOC enforces and reports
  - Customized dashboards can help!
- 
- **AIM for going beyond compliance**



# Assessment vs. Penetration Test

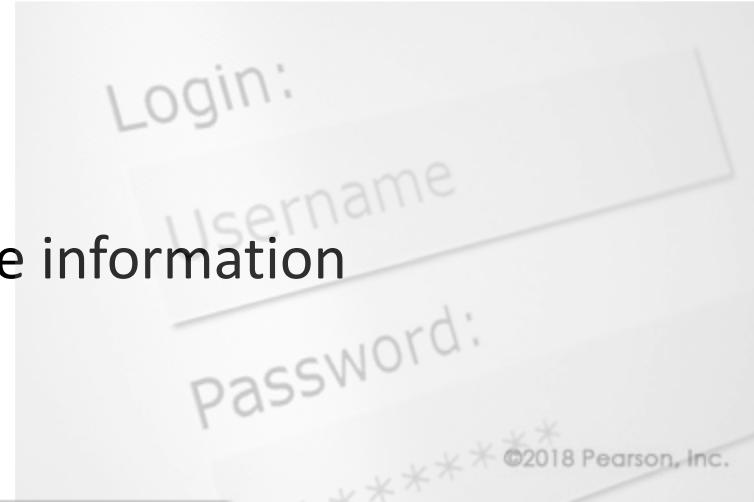
- **Assessment** – Using automated systems to identify potential vulnerabilities
- **Penetration Test** – Executing attacks against identified vulnerabilities

**Assessment is good to see your weaknesses**

**Penetration Testing is good if you know you are secure**

# Credential Scan

- **Host Scan**
- Less load on network (enumerated from local machine via commands like netstat)
- Considered “Safer Scan”
- **Only need Read-only access**
- Better data (more accurate)
  - Registry scan data and file attribute information
  - Behind personal firewall



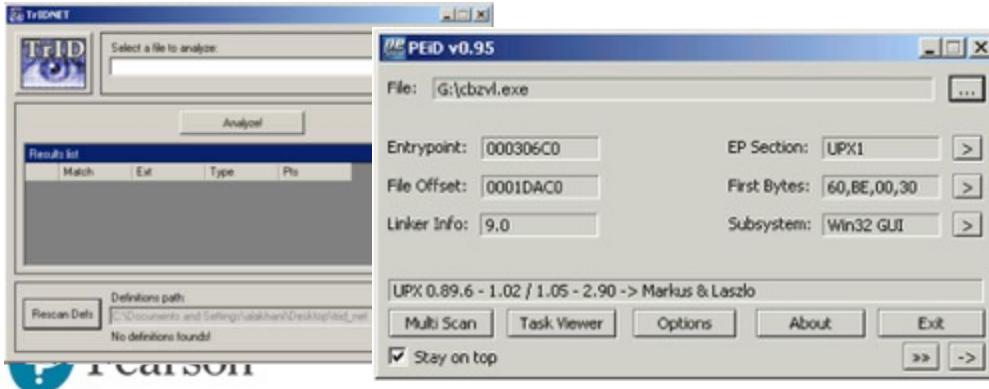
# Non-Credential Scan

- Network scan
- Similar to attacker viewpoint (external view)
- Relies on ports to return correct information about services running
- Potential false positives

**Key Concept:** Potentially more important vulnerabilities as these are what attackers would find first.

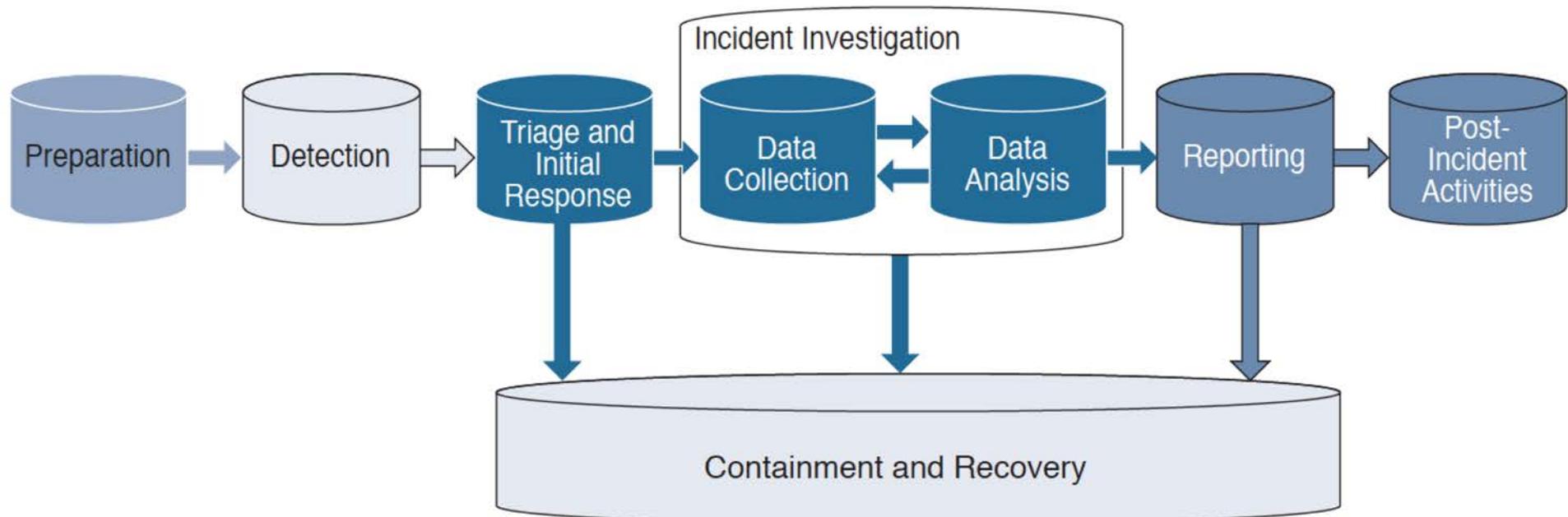
# Service 4: Analysis

- Analyzing various artifacts (TrIDNET / PEiD)
- Reverse Engineering
- Run time and dynamic analysis
- Vulnerability Analysis



# Service 5: Incident Management

Detecting and responding to security incidents or



# Security Incident

High

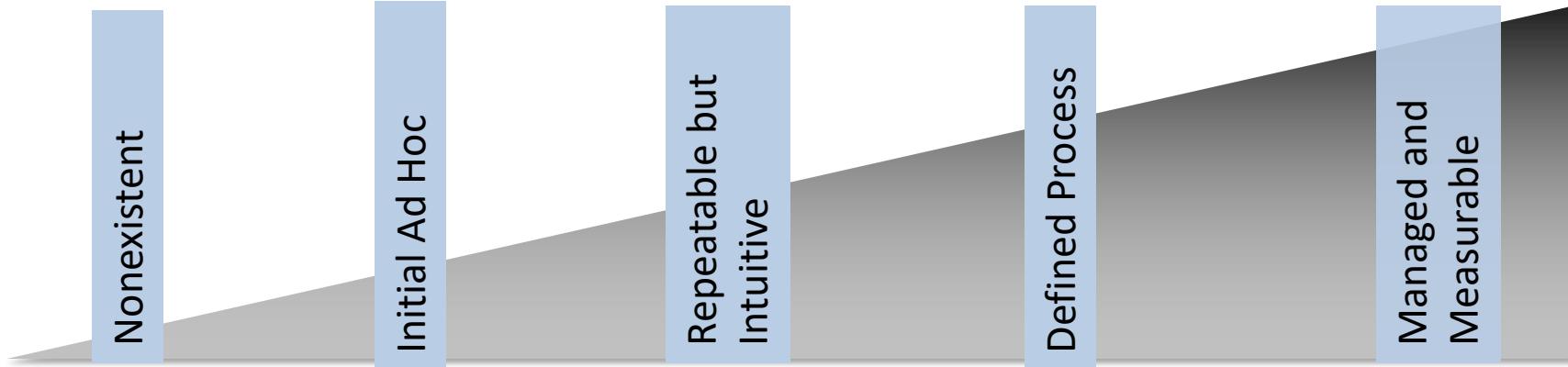
Incidents have server impact

Medium

Incident has significant impact

Low

Incident has minimal impact



# References for Incident Response

## FIRST CSIRT Framework

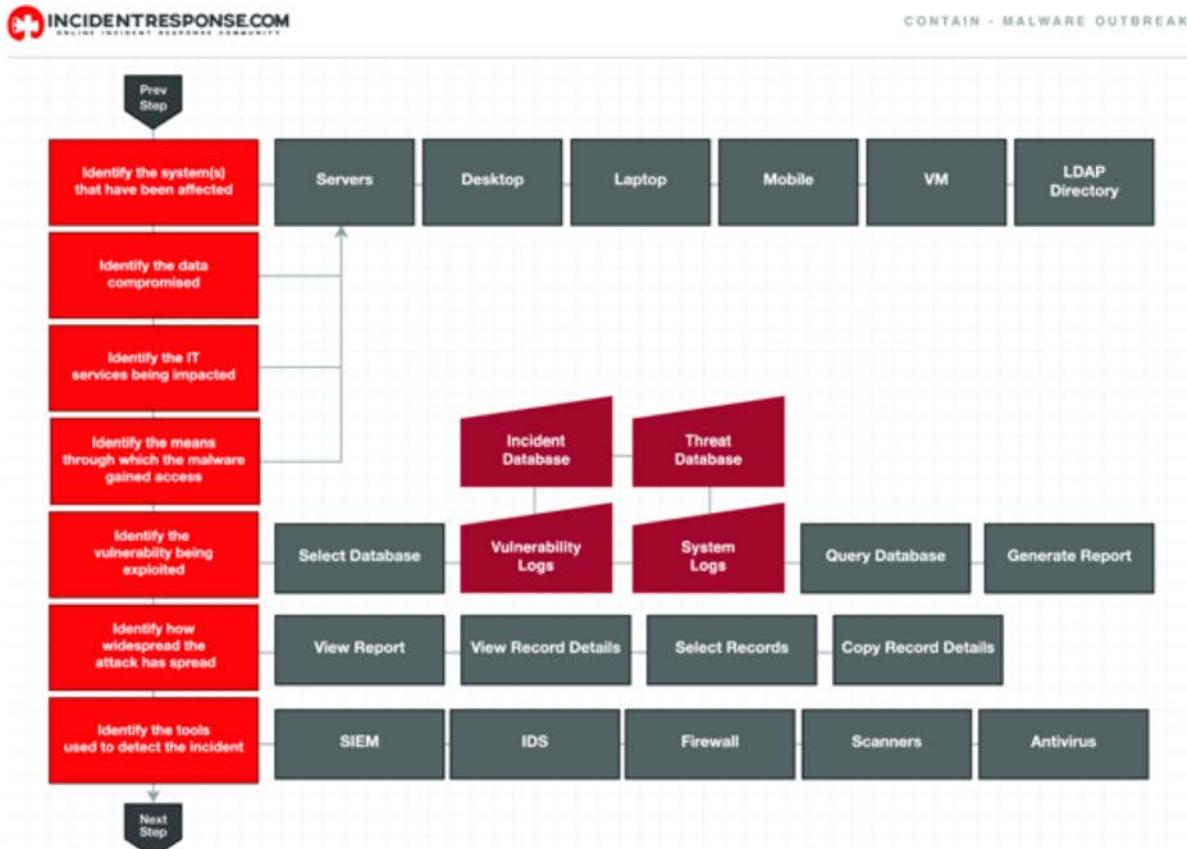
[https://www.first.org/education/csirt\\_service-framework\\_v1.1](https://www.first.org/education/csirt_service-framework_v1.1)

## PSIRT Services Framework

[https://www.first.org/education/FIRST\\_PSIRT\\_Service\\_Framework\\_v1.0](https://www.first.org/education/FIRST_PSIRT_Service_Framework_v1.0)

# Playbooks

<https://www.incidentresponse.com/playbooks/>



Security Information and Event Management – Centralized log collection from various tools to mine data and respond to events

Security Orchestration, Automation and Response – Collects data from a range of sources and automates response when possible

Endpoint Detection and Response (EDR)– Uses local detection and cloud capabilities to detect threats on endpoints

(XDR) – X represents multiple data sources to expand EDR. XDR is the future of EDR allowing for network, endpoint and cloud data.

# Service 6: Digital Forensics

- Understand what happened
- Collect evidence for potential legal action
- Support HR for evidence of internal complications



# Service 7: Situation and Security Awareness

- Training and education
- Understanding industry trending threats
- Policy advertisement
- Mentoring



# Service 8: Research and Development

- Work with stakeholders to educate about risks
- Understanding industry trending threats



# Managed Services vs Internal Pros

## Internal

- Knowledge of business
- Data stored internally
- Cross department correlation
- Tailored requirements

## External

- OPEX costs that can be spread out
- No conflict of interest
- Scalability and flexibility
- Leverage other customer trends

# Managed Services vs Internal Cons

## Internal

- Cost
- People (Hire / Maintain)
- Potential conflict of interest
- ROI concerns

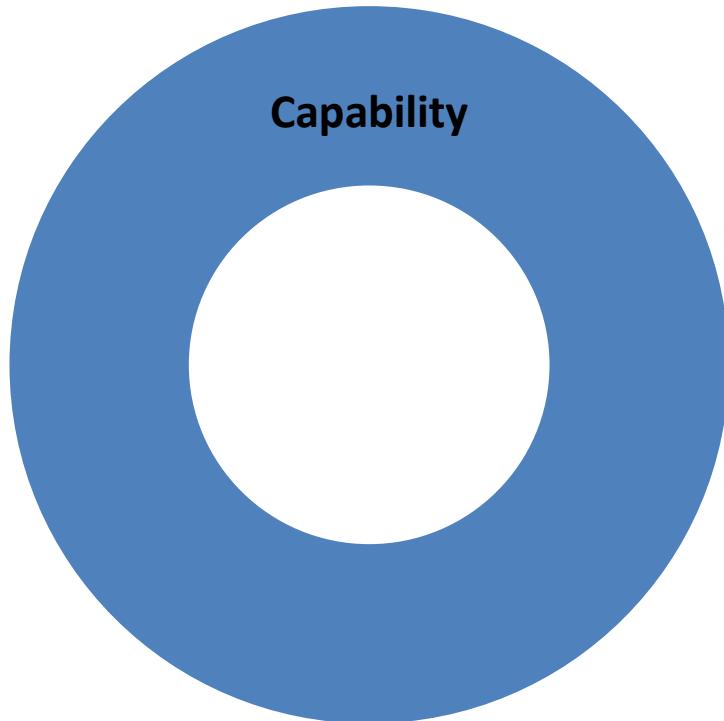
## External

- Limited business knowledge
- External tools and data flow
- Lack of communication
- Usually not detected people
- Limited customization
- Services are limited based on cost (Gold, Silver, Bronze)

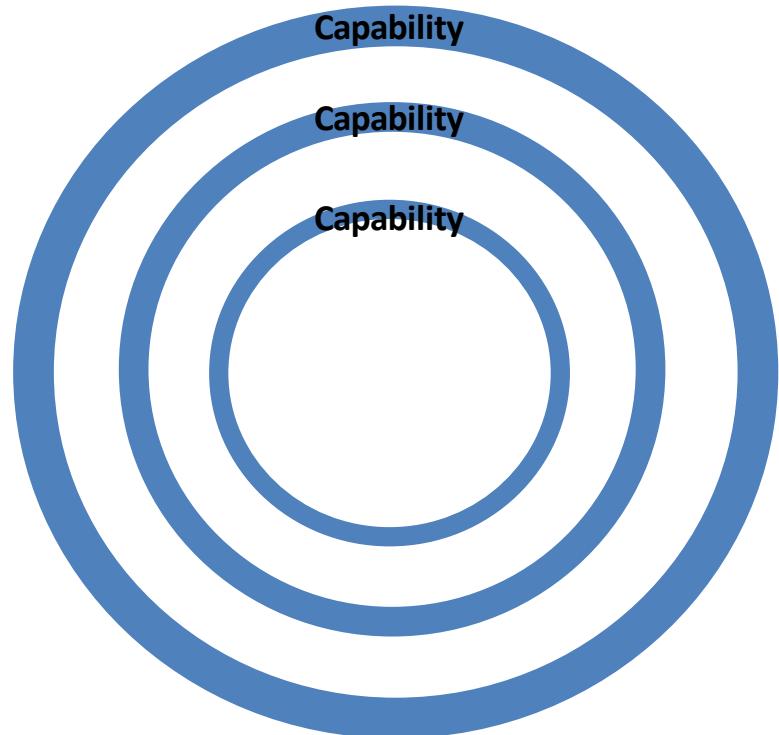
# Cyber Defense 101



# Best of Breed vs Defense in Depth



OR



# Defense in Depth

- Layering defenses
- Best practice use different capabilities according to kill chain
- Should apply to all areas of network

Firewall

Firewall

Firewall

= Weak

Firewall

IPS

Breach  
Detection

= Better

# Defense in Depth

- Leverage different security levels when using the same technology

Perimeter Firewall

**Trust 0 outside | 50 DMZ | 100 inside**

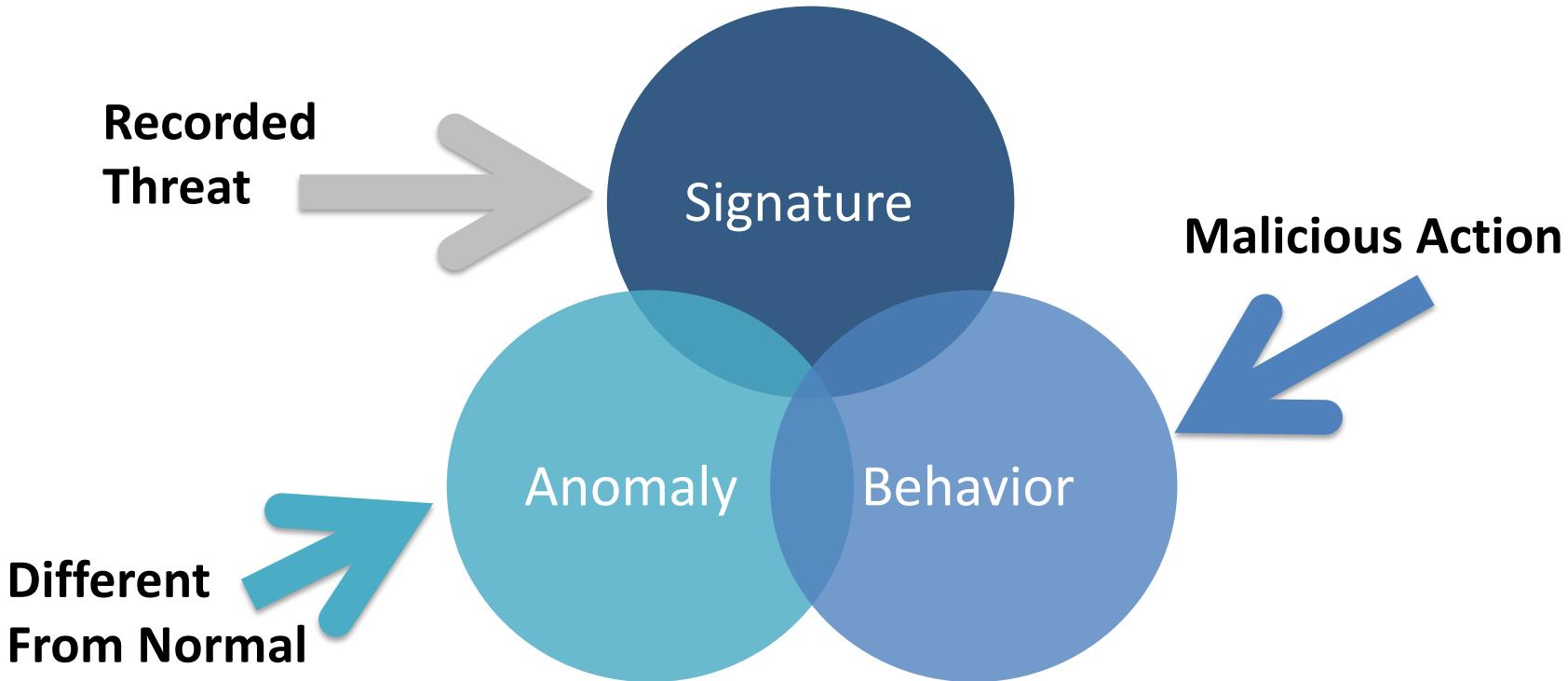
Internal Firewall

**Segment employees, HR, Guests, etc.**

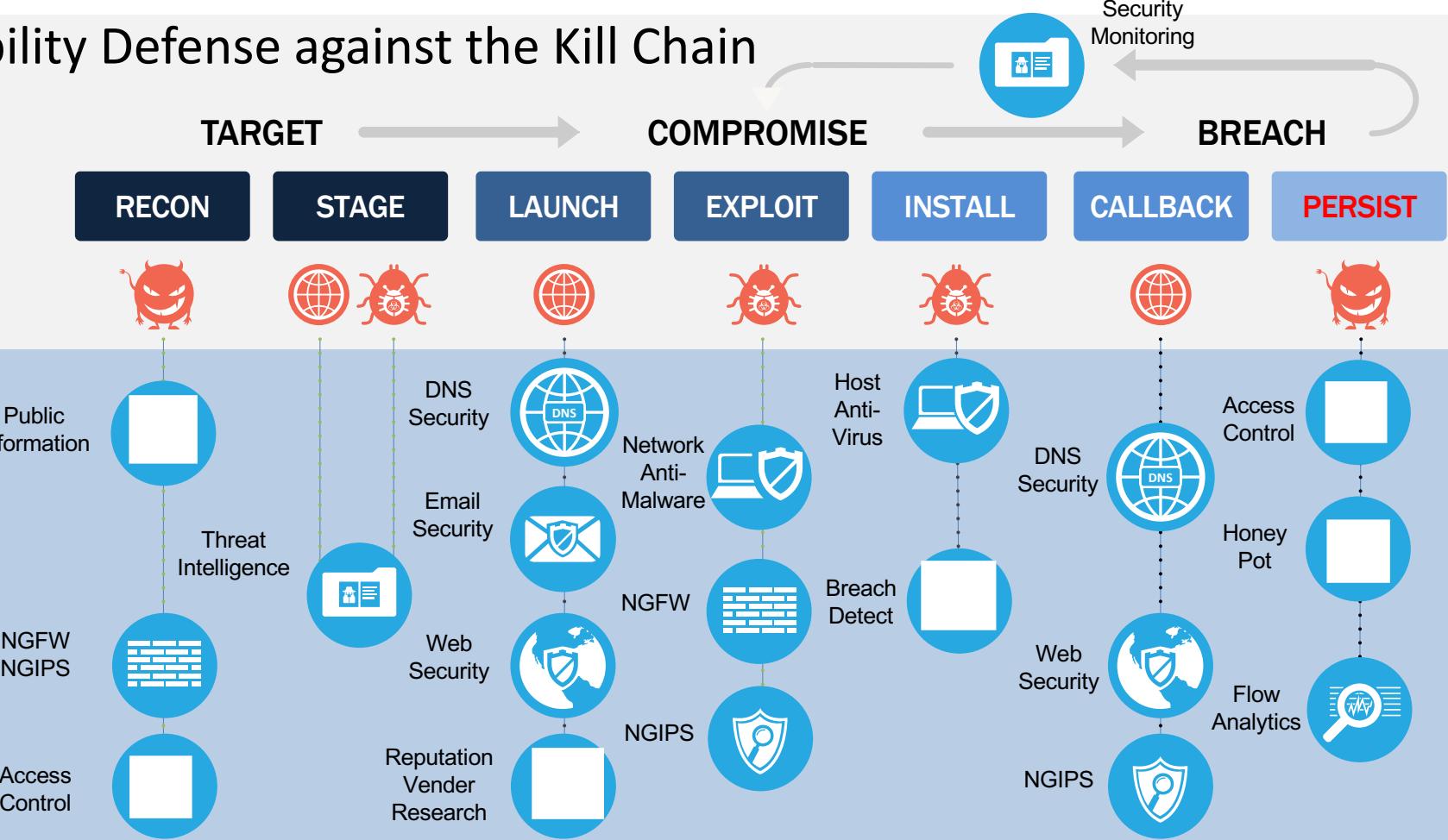
Data center Firewall

**Segment data center resources / applications**

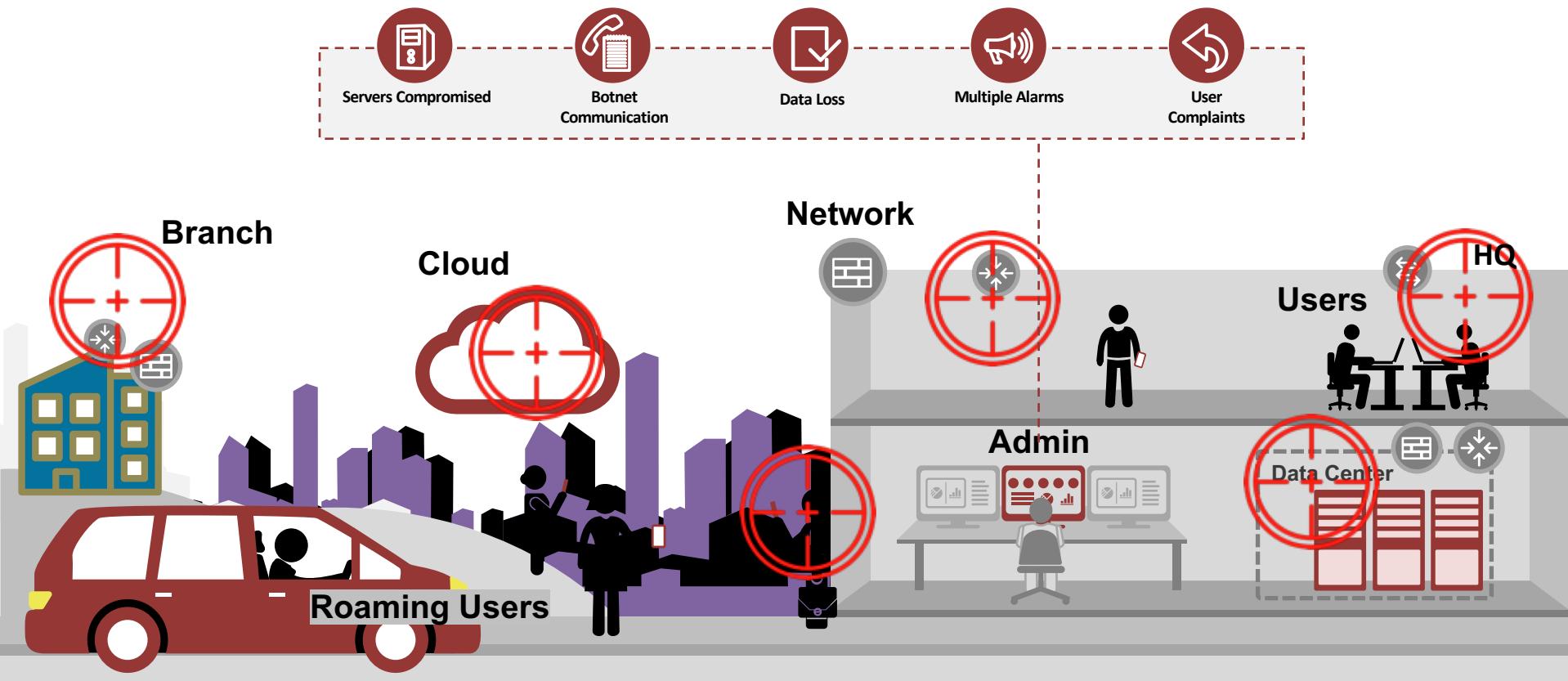
# Security Capabilities



# Capability Defense against the Kill Chain



# Many Targets to Consider



# Known and Unknown Threats

- **Known** – Attack has been seen and characterized
  - Develop signatures for detection
  - Behavior triggers
  - Domains blocked
    - Antivirus / IPS leverage this
  
- **Unknown** – Attack not known and characterized
  - Signatures do not exist
  - Behavior and anomaly detection focused
    - Breach detection / Sandboxing / Honeypots

# Whitelisting and Blacklisting

- Blacklisting – Blocking specific software from being installed
- Whitelisting – Prevents software that is not on a preapproved list
- Signature based – One specific threat

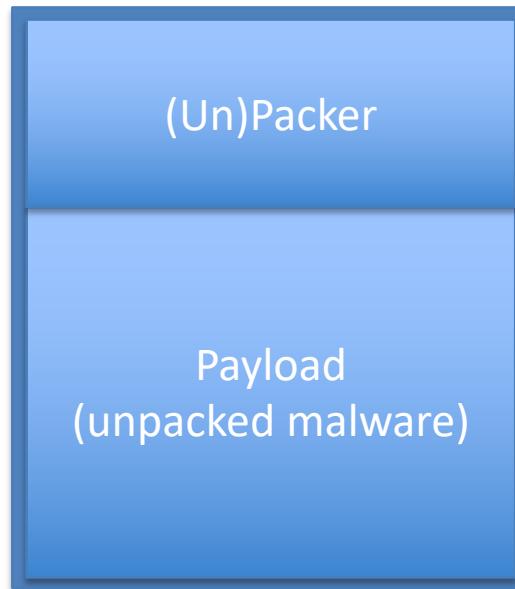
# Threat Intelligence

- Evidence-based knowledge, including context, mechanisms, indicators, implications and actionable advice about an existing or emerging threat
- Think what “Other Networks” are seeing

Example: Other company data warned us about evil.exe and now raised to a critical threat when seen on our network

# Packing Malware 101

Bypass signature based detection



Frequently Changed

Changed Less  
frequently

# Maintaining Malware Is a Fulltime Job



**Coder Team**  
3 group members  
6AM-8PM GMT  
Mo-Fr\* (Su)



**Packer Team**  
9 group members  
~10AM - 10:30PM GMT  
Mo-Sa\* (Su)

**Developing and maintaining malware and a malicious infrastructure is a full time job !**



# Senna Spy One EXE Maker 2000 - 2.0a

Official Website: <http://sennaspy.tsx.org>

e-mail: senna\_spy@hotmail.com

ICQ UIN: 3973927

Join many files and make a unique EXE file.

This program allow join all kind of files: exe, dll, ocx, txt, jpg, bmp ...

Automatic OCX file register and Pack files support

Windows 9x, NT and 2000 compatible !

Short File Name	Parameters	Open Mode	Copy To	Action
CALC.EXE		Hide	System	Open/Execute
ROOTKIT.EXE		Hide	System	Open/Execute

Add File

Delete

Save

Exit

Command Line Parameters:

Open Mode

- Normal
- Maximized
- Minimized
- Hide

Copy To

- Windows
- System
- Temp
- Root

Action

- Open/Execute
- Copy Only

Pack Files?



Copyright (C), 1998-2000, By Senna Spy



Pear

# Security Best Practices

- Scaled For Security Maturity -

TIME



Edge Defense



Host Defense



Access Control  
and Segmentation



Insider Threat and  
Continuous  
Monitoring



# Edge Defense



**Edge Defense**

# Edge Security Technologies

- **WAF** – Web application firewall for application / layer 7 attacks
- **Firewall / NG Firewall** – Permit and deny traffic. Also physical segmentation
- **IDS / IPS** – Detect and prevent attacks
- **DNS** – Prevents connections to malicious sources
- **Reputation / Threat Intelligence** – Threat data from other networks.
- **Proxy** – Mask system data

# Firewall 101

- **Packet Filter** – Simply checks the characters of each packet against firewall rules
- **Stateful Inspection** – Beyond packet filters also viewing state of connection. (What today's standalone firewalls do)
- **Next Gen** – Beyond stateful including applications, users and context
- **Web Application Firewall** – Specialized for web application attacks such as SQL injection and cross site scripting

# Proxy vs. Application Layer Firewall

## Proxies

- Internet bound ports (80, 443)
- Cache traffic
- Higher performance (example HTTPS decryption)

## Application Layer Firewalls

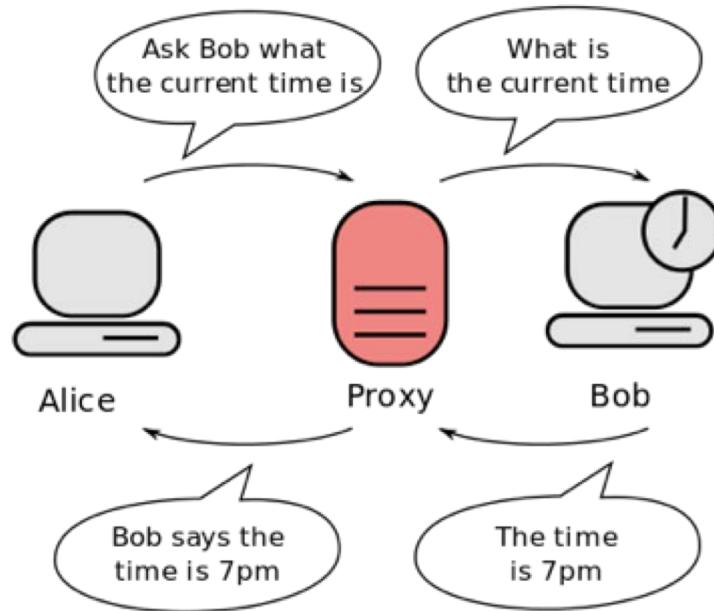
- All ports and protocols
- View near real time traffic / no cache
- Typically part of “Next Gen” platforms



- Both typically offer security detection and content filtering capabilities
- Security value depends on model and installation

# Intercepting Messages - Proxy

- Display and modify HTTP and WebSockets messages that pass between the proxy clients and web server.



# Types of Proxies

- **Open Proxy** – Accessible by anybody on the Internet
  - Can conceal user IP
  - Typically done directly from host or using WCCP routing
- **Reverse Proxy** – Proxy appears to clients as ordinary server. Requests are forwarded to one or more servers, which handle requests
- **Man-in-the-middle** – Attacker captures traffic via ARP poisoning, going in-line, DNS spoofing, STP mangling, etc.

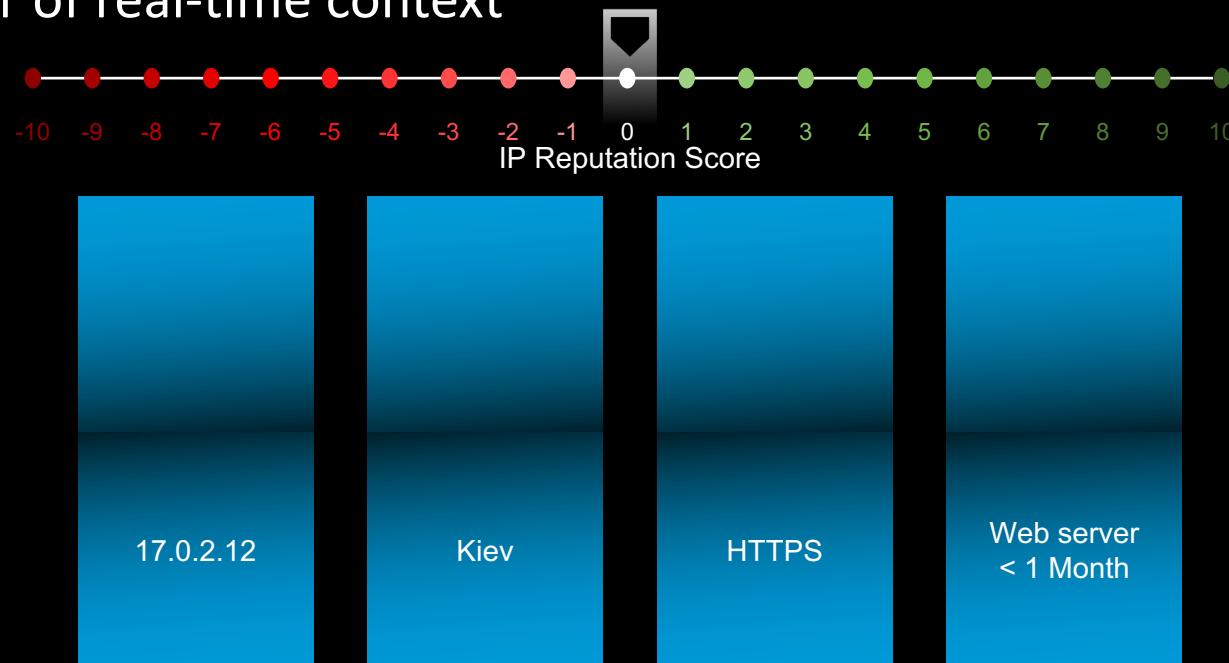
# Web Application Firewall WAF

- All ports and protocols
- View near real time traffic / no cache
- Typically part of “Next Gen” platforms
- Sometimes called UTM (with other features)

Palo Alto – Cisco Firepower – Checkpoint - Fortinet

# Reputation Analysis

The power of real-time context



010 10010111001 10 100111010 000100101 110011 0110011101000011000  
0101 1100110 1100 111010000 110 0001110 00111 010011101 11000 01111  
0010 010 10010111001 10 100111010 00010 0101 110011 011 001 1101000011000

1010011101 1100001110001110 1001 1101 1110011 0110011 101000 0110 00 0111000 111010011 101 1100  
100 0111010011101 1100001110001110 1001 1101 1110011 0110011 101000 0110 00 0111000 111010011 101 1100

# Reputation Analysis

# The power of real-time context



## Who

## Suspicious Domain Owner



## Where

## Server in High Risk Location



# How

Dynamic IP  
Address



## When

Domain  
Registered  
< 1 Min



010 10010111001 10 100111 010 000100101 110011 011001110100001100  
0101 1100110 1100 111010000 110 0001110 00111 010011101 11000 0111  
00010 010 10010111001 10 100111 010 00010 0101 110011 011 001 1101000  
1010011101 1100001110001110 1001 1101 1110011 0110011 101000 0110 00  
01 1101 1110011 0110011 101000 0110 00 0111000 111010011 101 1100  
100 0111010011101 1100001110001110 1001 1101 1110011 0110011 101000



Dear valued customer of TrustedBank,

We have received notice that you have recently attempted to withdraw the following amount from your checking account while in another country: \$1:

If this information is not correct, someone unknown may have access to your account. As a safety measure, please visit our website via the link below to verify your personal information:

<http://www.trustedbank.com/general/custverifyinfo.asp>

Once you have done this, our fraud department will work to resolve this discrepancy. We are happy you have chosen us to do business with.

Thank you,  
TrustedBank

Phishing

## Click Jacking

Feb 2, 2012 8:50 PM

Apple is looking for iPhone 5 testers! The first 1000 users that go to <http://celltestandkeep.com> and enter code 7923 will get to test & keep a new iPhone 5



Dear valued customer of Trusted

We have received notice that you  
following amount from your che

If this information is not correct,  
account. As a safety measure, please  
your personal information:

<http://www.trustedbank.com/get>

Once you have done this, our records  
discrepancy. We are happy you

Thank you,  
TrustedBank

## Phishing



## Click Jacking

and enter code 7923 will  
not to test & keep a new  
information

## Botnets / Worms



## SECURITY THREAT DETECTED AND BLOCKED

WW

DM

Based on Cisco security threat information, access to the web site <http://ihaveabadreputation.com/> has been blocked by the Web Security Appliance (WSA) to prevent an attack on your browser. The Cisco Security Intelligence Operations (CSIO) Web Reputation Score for this site indicates that it is associated with malware/spyware, and poses a security threat to your computer or the corporate network.

In order to cater for a growing number and variety of devices on the Cisco network, malware protection has shifted from the endpoint, deeper into the network. In order to offer the most effective protection to computing assets on the Cisco network, CSIRT and Cisco IT jointly rolled out the Cisco Ironport WSA solution on all Cisco Internet Points of Presence (IPoPs). These WSAs are configured to block access to sites whose Web Based Reputation Score (WBRS) shows that they are serving malware or content otherwise harmful to users of the Cisco corporate network.

If you believe this page was incorrectly blocked, please open a [case](#) with Infosec, providing the corresponding debug information below, and an analyst will determine whether the block was due to a misclassification. Please note that Cisco Infosec does not add sites to the WSA allowed-list on demand, and may require the end-user to contact [Senderbase](#) directly in order to submit a request to have a site removed from the WSA blocked-list.

Debug information to include when opening a case:

Date:	Thu, 09 Oct 2014 17:35:41 GMT
Time:	1412876141.450
Client IP address:	10.118.14.120
Request URL:	<a href="http://ihaveabadreputation.com/">http://ihaveabadreputation.com/</a>
User-Agent:	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_5) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/38.0.2125.101 Safari/537.36
Transaction ID:	0x1a4300e9
Request Method:	GET
Blocking reason:	BLOCK-MALWARE
Web Reputation Score:	-9.5
Malware threat name:	
Malware category name:	
Web reputation threat reason:	Researchers or users identified possible threats.
Web reputation threat type:	othermalware
Proxy hostname:	rtp5-dmz-wsa-1-mgrnt.cisco.com

For more information about Cisco security, visit [Cisco.com/Security](#).

As a matter of good practice, you may check whether your browser or any component plugin is vulnerable by visiting [browsercheck.qualys.com](#). The UID at the end of the browsercheck.qualys.com URL does not uniquely identify your machine to Qualys; it is a shared UID to group all requests originating from Cisco IP ranges.

## Details for www.movies123.com

One or more of the IP addresses that this domain resolves to are currently blocked by Umbrella: 208.73.210.200

## Identify Malware



## Identify Source



## Associated Samples

POWERED BY CISCO AMP THREAT GRID

Threat Score	SHA256 Signature	AV Result
100	12eac147dbc632b29feef44f882530022c25e99156e689d8450740c92bc18a7d	
100	27ef0b34d05c50f2b3071a1909ac9588d8020123d0566980c4b482929632f1b	Win.Virus.Sality, Win.Trojan.Agent
100	5667ba55ba145a621564539e9e958278a25e7d4198f58fa1c3137fa430c6a69	Win.Trojan.Ramnit
100	5d5d971dc39bccb48901ad6ec32263ac16f9503777cde01071104a2d1c759e2ba	
100	8c1383005a9986204422e221ac5a1460103cfb0c9d817b8f950063ecd077a6d	
100	c3552cd1a1200ee6210146d598066439c3ad1f736020108a540950449440e11	
100	d265745e1a3ee8f52920aa413a0050eabff9609a211881bca3794eef3f2671d	
100	db4a0c25480093ce453e9eca819d564635eab02e0857e35d8e0183d1c143d	Win.Trojan.Ramnit
100	e47bf85d1f2522405a90277380b30793c5a2c02424d27d8cb02292a472bd	
100	f0678671926b4d5d25af1dd32dc6bc4ea71cbe20c488bcb181b42c5e9f5386	

1-19 &lt; &gt;

Crown domains hosted by 208.73.210.200

all.qents.com app0.com qents.com cocolive.com imap.qents.com www.lowpricehouse.com web.qents.com www.app0.com mx.qents.com mydeed.com  
 mpauth.qents.com www.cocolive.com paysheet.com www.qents.com lexberg.com chinaphoneshop.com smrt.qents.com huc.com lowpricehouse.com  
 com.0rz.com 1-teens-sex.com 1044.com t-bodies.com 1212.vn.com 123act.com 13p.com 165.agilecodersapp.com 172k.com 185.adamayeve.com 19.2  
 daycore.com facebook.com 1f.com top.com 1stfinancial.com 2229933.com 2244.com 226.bambulove.com 236.anewexperience.com 2425.com 248.b  
 252.bensonmarcom.com 2d.com 29ex.com 3.exchange2010.livemail.co.uk.ausoe.com 33556666.com 35wsee.com 3estudio.com 3js.com 3w.com  
 391.com 4889388.com 4amazinggirls.com 4cs.com 4litalschools.com 4richels2.com 4tel.com 4seo.com 4x4searchersvideo.com 5.aluminumrolling.co  
 1car.com 52yyx.com 54.ado.co.in 56.bestchristmascarols.com 5names.com 66.bandirequest.com 6611889.com 71.amortizationloans.com 7852488.com 7daysinla.com  
 .com 8855.com 8877.com 8t@www.com 91.chinesesay.com 95.anchorgeatackanees.com 9997878.com fdkkwz.polo.hangoutatome.com 9monthsinstyle.com  
 1702.g.akamai.net.akamai.net.autoe.com aaaa.com abacorsort.com aboutoliedisease.com aboutmarketingmix.com aboutwebsite.com abuion.com  
 accountantslawyerscolorado.com accounts.betterhomehealth.com accountssolutions.com accuweather.com aceladharvaranacortes.com acsecurityinc.com achangedofheart.com  
 chor.com acnetreatment.exploreoffers.com acost.com acousticpassport.com activeight.com activepassive.com actives.com activation.com acun.com action.com  
 adam.feelingfit.com adammanley.com adki.onresalehome.com admin-hr-pc-1.familyhealth.com admin-pc.baoloc.com admin.screenactors.com adon.com  
 dcentrehospitals.com.net.in adsense100kblueprint.com adserver.yexlabz.com.net.in adsl.viettel.vn.com adult-free-host.com advancehotel.com adventuremantrailing.com  
 advertisingbanners.com aerotic.com aerhtsystems.com aero.com afamlymngage.com affiliatepayments.com afghantrade.com af.co.in atrictravelcentre.com agarz.io  
 girl.com agrienteomorrow.com ahlaw.com aimforbetterhealth.com aimslab.com airportsindia.com airtelbroadband.com ajdesigns.com akthomas.com  
 alamocares.com alaroreficeandcompany.com alaskahearthproducts.com alaskapersonalinjuryattorney.com alecplover.com alaxyinne.com althuttmotors.com alaga.com  
 als.hotpop.com aliyagallery.com alikay.com all-free-nude-old-granny-mature-women-xxx-porn-pics.com allegany.com alienxseanews.com allorthopaedics.com alpafid.com  
 properties.com allsearchengines.com aliteenblog.com alpha.jurix.com alphacub.com alphaind.com alphaleaf.com alphatecmg.com apigasten.com atarin.com  
 mastery.com amateurbootcamp.com amateurpomclips.com amazinghomes.com amazoncom.com ambercoast.com ambientsoho.com amei.com americashealthchoice.com  
 neexample.com angel.co.in angelaperson.com angeloleo.com angelsworkearth.com animal-kid.com animelink.com animelink.com animetpus.com animot.com annunciateprofil.com  
 ansnursing.com ansnursing.com answerly.com anweb.com apol.com apolive.com aoms.com aorshowroom.com ap-sonar.sociomatic.com.net.in apacboxes.com  
 pacjunctionflowershops.com apsanj.com aparthotels.com apartmentproblems.com apartmentintucson.com ap.co.in apgcars.com api.flx2.com api.ozmb.com  
 pthumbcreator.com apil.webtob thumb.com apkmovies.com apshop.com apotek.com appoxie.com applicous.com apprehensively.com apuca.com arabahq.com  
 arabsassy.com aramak.com archdass.com archiveachievypacvacationrental.com areaicode978.com aremena.com arta.com arashahr.com arizonafenclosedhomes.com

## Associated Websites



# Intrusion Detection and Prevention

**Signature Detection** – Looking for known attack patterns

**Threat Detection** – Looking for malicious behavior

**Anomaly Detection** – Looking for unknown or unusual behavior

**Intrusion Detection System** = Passive (can't block attacks) and can be inline or off mirror port

**Intrusion Prevention System** = Can block attacks and must be deployed inline

Can be host (software) or network (appliance / virtual)

# Why Tuning Matters



# How Effective Is Your Prevention Technology?



Systems + Applications



Websites Accessed

*Integrating Security with  
Vulnerability Scanning  
and  
Prevention  
understanding  
the network!!!!!!*

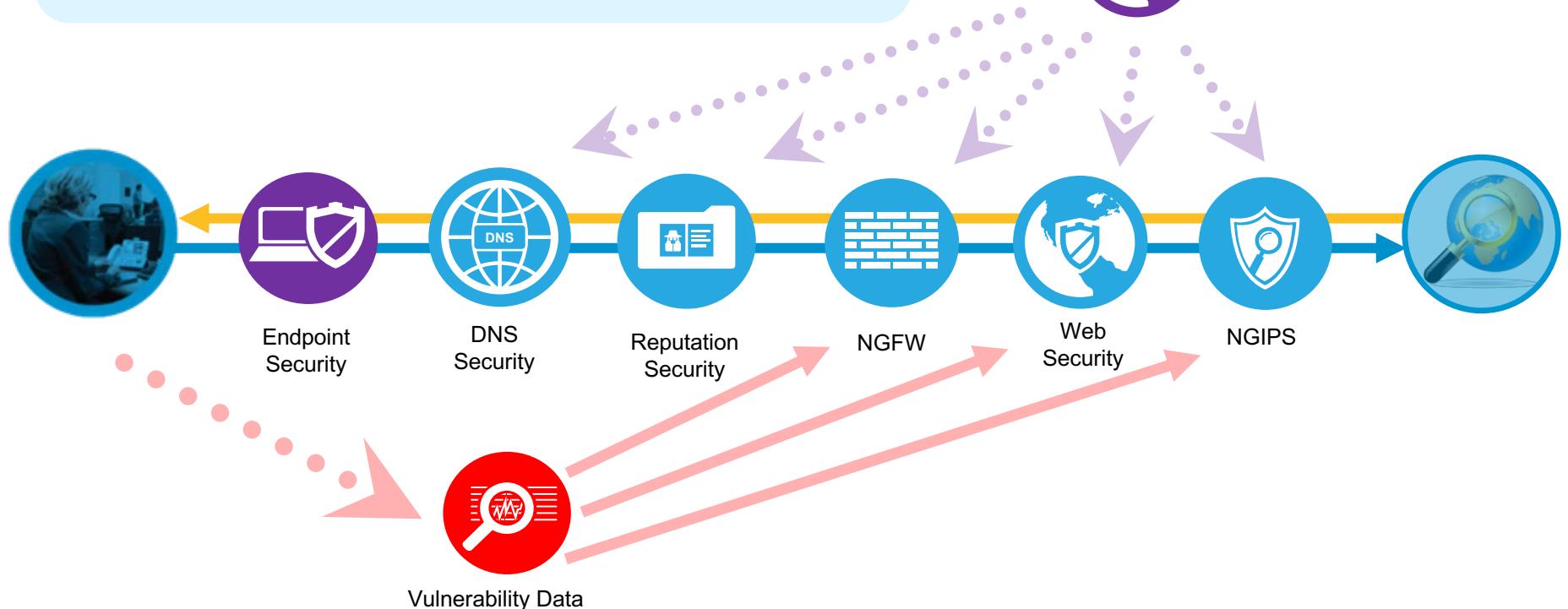




# Defending the Perimeter - Better

- Everything starts with DNS
- Application Layer Firewall or Proxy for all layer protection
- Reputation analytics reduces attacks
- IPS for blocking attacks
- Continuously evaluation for vulnerabilities and updating signatures

# Perimeter Best Practices





# Host Defense



# Protecting Endpoints

- **Hardened Configuration** – Disable unnecessary services
- **Patch Management** – Close vulnerabilities
- **Group Policy (GP)** – Pushing security policy to many endpoints
- **Endpoint Security Software** – Antivirus, host IPS, etc.
- **Password Policies**
- **Host Firewalls**
- **File Integrity Checking** – Notifies changes in files



# Permissions

**Least Privilege** – Only rights needed to do job

**File Permissions** – What people can or can't access

Example: Chmod 777 –Rv = anybody can do anything

**Centralized Account Monitoring** – Why is Joey logging in from China and Canada within minutes?

# Antivirus

**File Base Signatures** – Known malicious files

**File Behavior** – Some file analytics

**File Modification Detection** – Limited encoding detection

**Typically older threats** – Trojans, viruses, and worms

**Targets KNOWN threats with Signatures**

# Antimalware

- Protects against infections caused by malware, viruses, worms, Trojan horses, rootkits, spyware, keyloggers, ransomware, and adware
- Typically more complete than antivirus (newer threats)
- May be called **File integrity** solution or **breach detection**

**Virus** – Code capable of copying itself and damages computer

**Malware** – Umbrella term for various malicious software

# Host IPS

**Signature Detection** – Looking for known attack patterns

**Threat Detection** – Looking for malicious behavior

**Anomaly Detection** – Looking for unknown or unusual behavior

- **Typically deployed with Anti-Virus and other bundles**
- **Best Practices** – Share threat data with network IPS

**Exam: Make sure question isn't Anti-Virus before selecting Host IPS**

**McAfee – Sophos – Symantec – ClamAV – etc.**

# Endpoint Best Practices

Threat Intelligence



Mobile Device Management  
Host Management Software

Anti-Virus  
Known Threats

Anti-Malware  
Unknown Threats

Reputation  
Security

VPN

Network  
Security

Web  
Security

Vulnerability Data





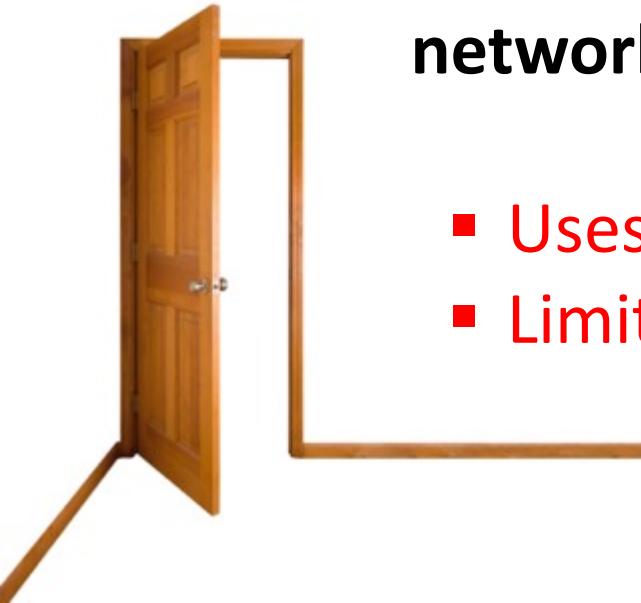
# Network Access Control



**Access Control and  
Segmentation**

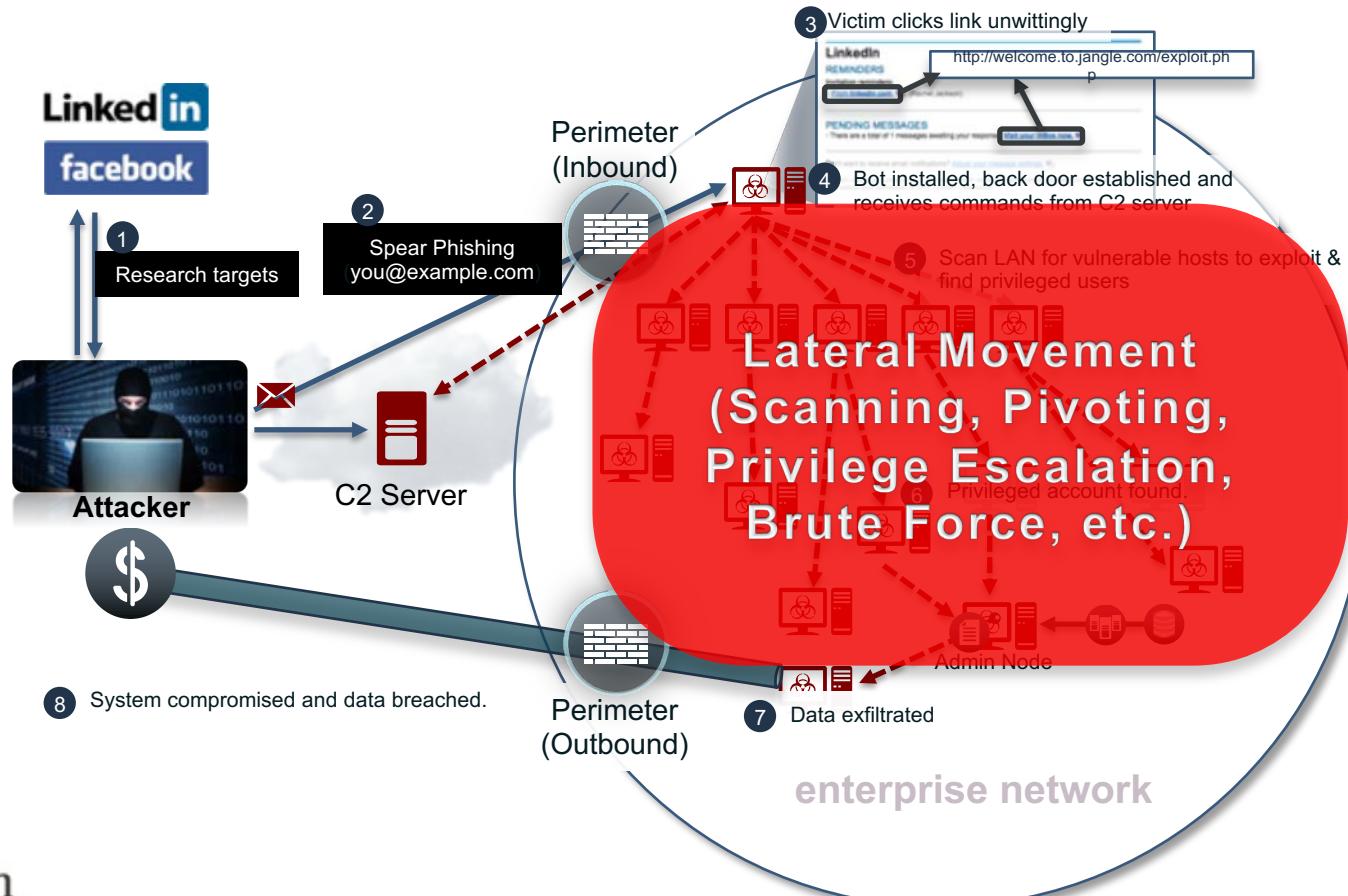
# Access Control

- **Basic concept** – Evaluate systems that access the network
- Typically not focused on systems **on the network**

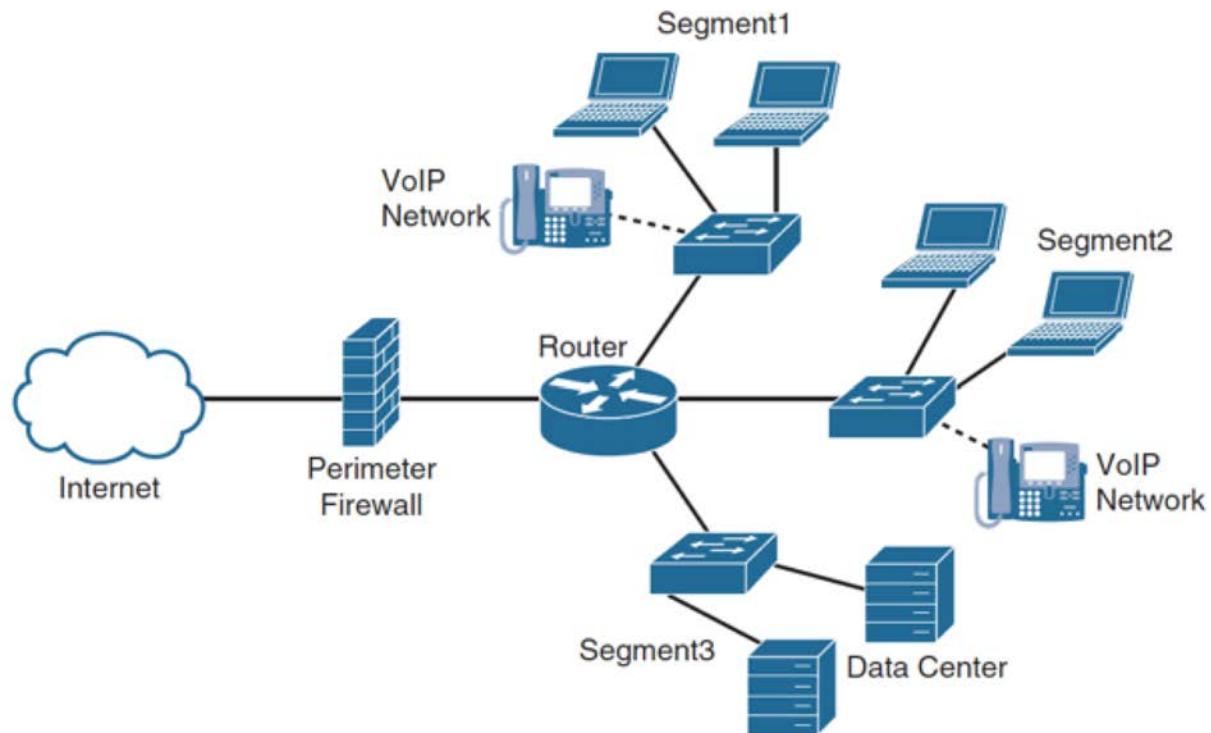


- Uses other technology (IPS, Breach)
- Limited inside visibility

# Lateral Movement (Without Segmentation)



# Segmentation



Physical Segmentation

Virtual Segmentation

Separate Firewall Contexts

Virtual LAN (VLAN) Segmentation

Access List Segmentation

SGT (Packet Level) Segmentation

# Access Control Remediation / Eradication

- **Quarantine** – Limit or deny network access
- **Isolation** – Put into a separate VLAN or take off the network to limit risk
- **Patch / Upgrade** – Windows / AV update
- **Software Link** – Offer software

# Identity Key Concepts

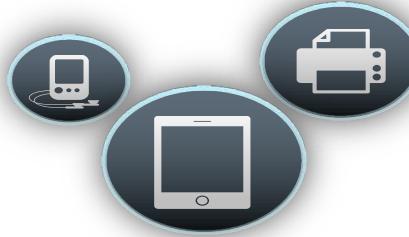
- Authentication – Who are you?
  - Authorization – What can you access?
  - Accounting – Record what you do
  - Common called AAA
- 
- Multifactor – Using different things to prove identity
  - Centralized identity and access management (IAM)
  - Directories – Control access level (example LDAP)

# Profiling



## Active Scanning

ISE collects device data to determine what it is.

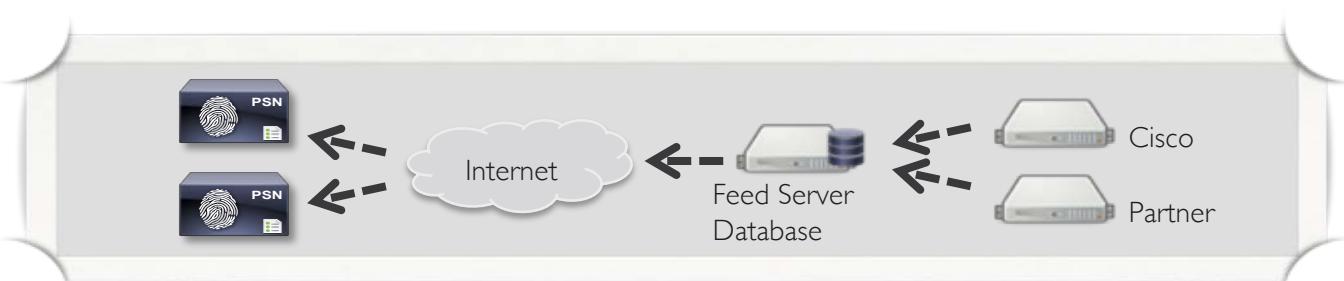


## Integrated Scanning

Cisco Wireless Controllers & Switches offer integrated device profiling\*

## Device Feeder Service

New content dynamically added.



# Posture



ISE can isolate non-compliant host and attempt automatic remediation of issues.



Dynamically Updated Posture Content

# Network Access Control Best Practices



Control who gets onto your network



- Who are you? → Raylin



- What Device? → BYOD or Corporate Endpoint



- Where are you? → Building 200, 1<sup>st</sup> Floor Lobby



- When? → 11:00 AM CST on April 10<sup>th</sup>



- How ? → Wired, Wireless, or VPN



ISE



Wired

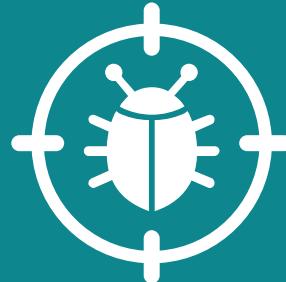


Wireless



VPN

# Breach Detection

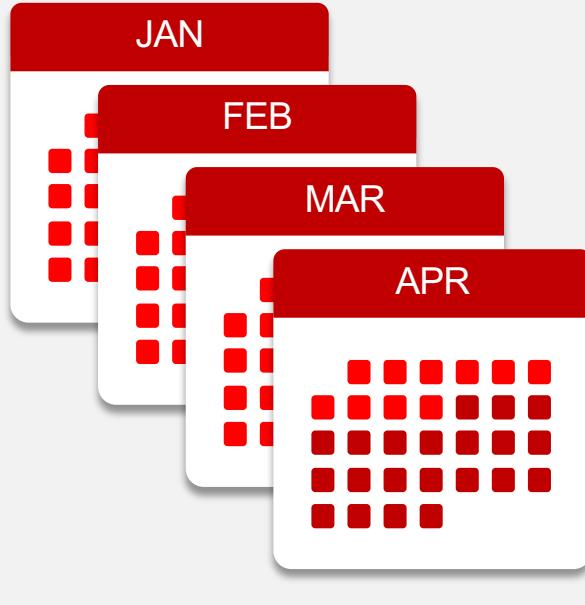


Insider Threat and  
Continuous Monitoring

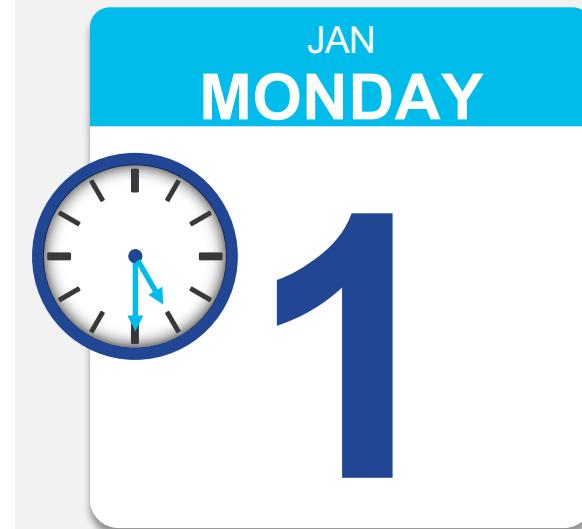


# Detect infections earlier and act faster

**Industry TTD rate:<sup>\*</sup> 100 days**



**Cisco: 17.5 hours**



- Automated attack correlation
- Indications of compromise
- Local or cloud sandboxing
- Malware infection tracking
- Malware analysis

# Common Historical Data

## **PCAP** – Logging network data

- Example: Listening to phone calls
- More storage / More details

## **NetFlow** – Logging network records

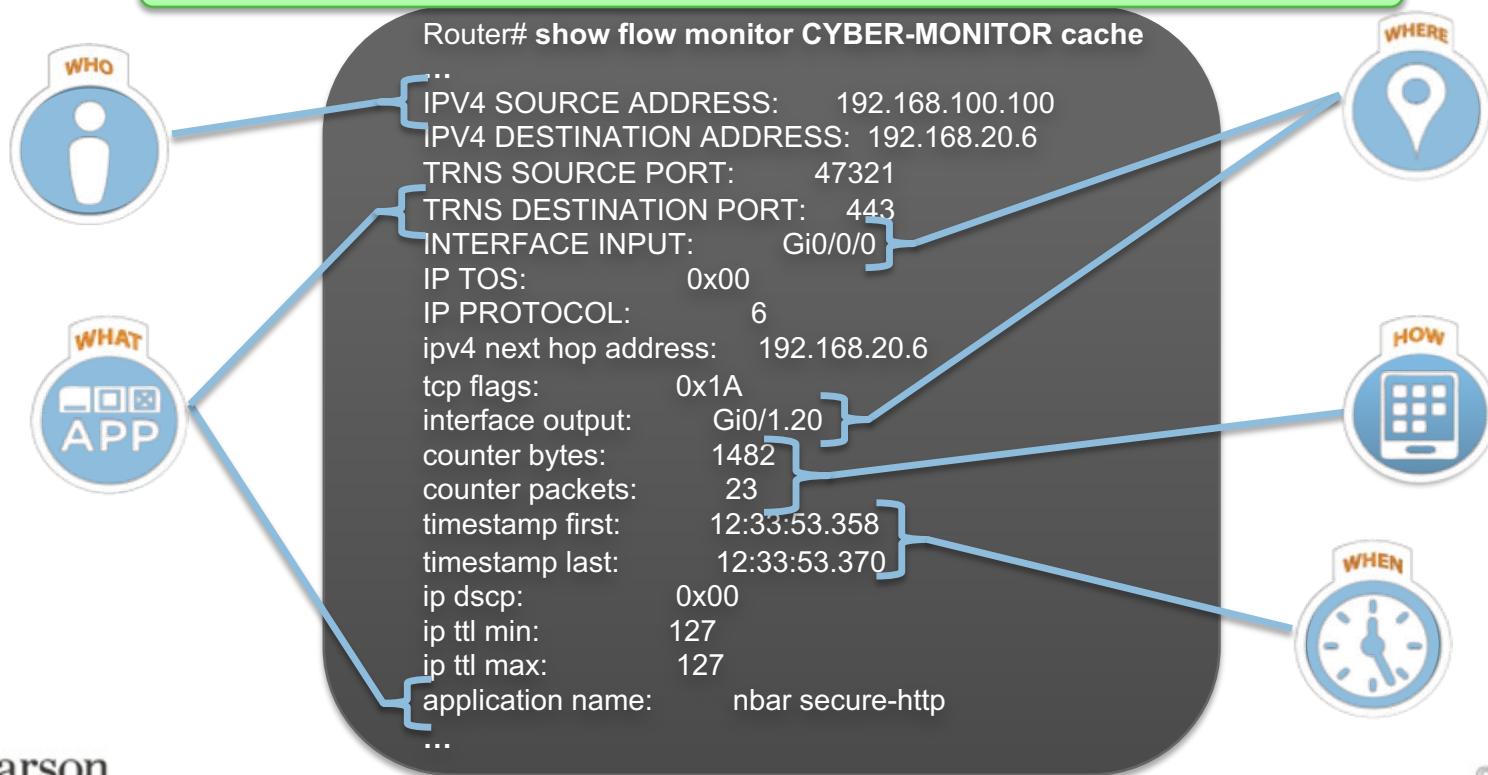
- Example: Looking at details of phone call
- Less storage / Less details

# Network Security Technology

- **Firewall** – North South / East West
- **Content Filters / Application Layer Firewalls** – User / Application Data
- **Access Control** – Who and what is accessing network
- **IPS/IDS** – Signature and some behavior detection
- **Honey Pot** – Monitor traps
- **NetFlow** – Leverage network traffic for indications of compromise
- **Network Baselines** – Tools used to verify normal and unknown traffic

# NetFlow = Visibility

A single NetFlow Record provides a wealth of information



# Why Unsampled NetFlow?



## Sampled NetFlow

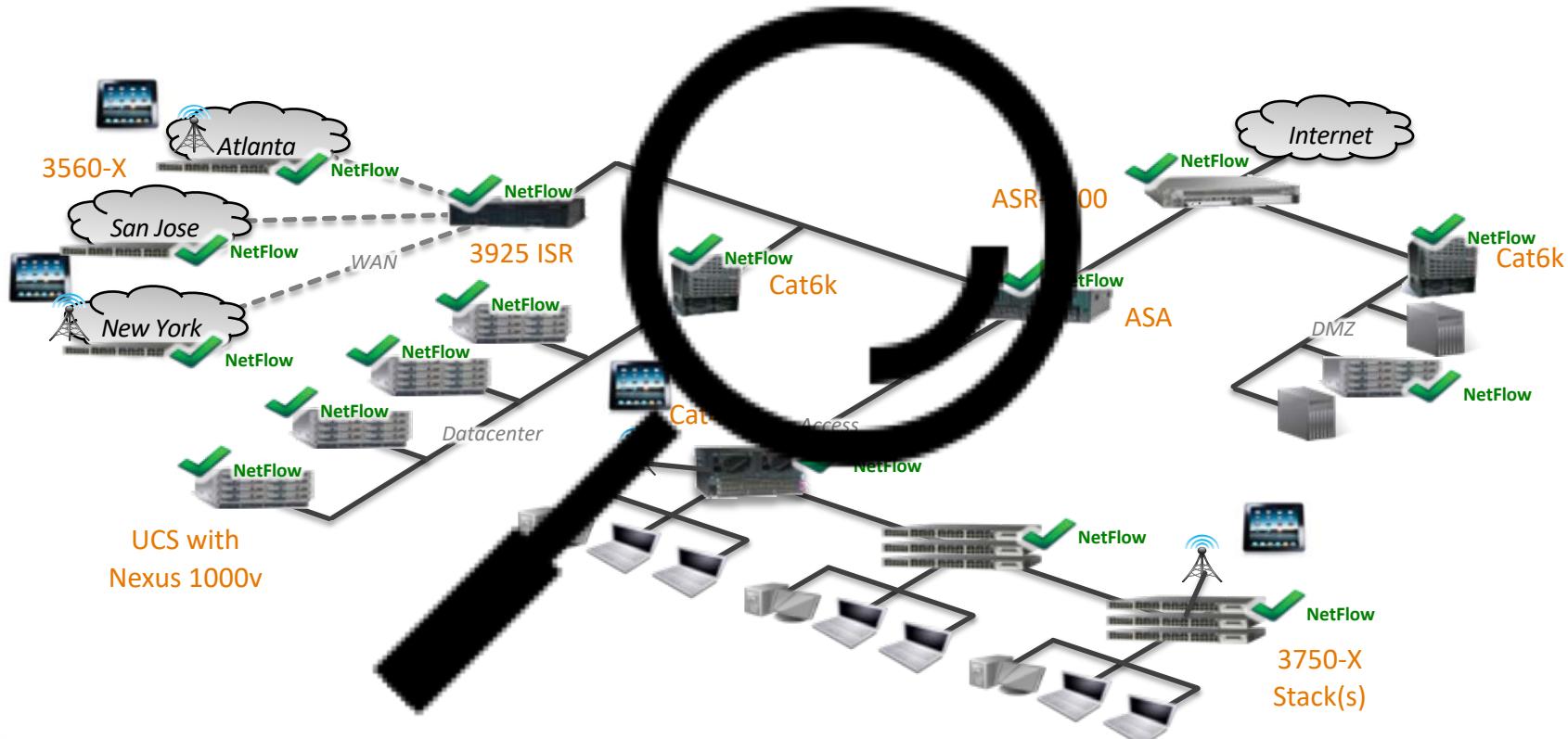
- Subset of traffic, usually less than 5%,
- Gives a snapshot view into network activity
- Similar to reading every 20<sup>th</sup> word of a book
- Suitable for detecting large scale DDoS attacks, but not extended, slow attacks



## Full NetFlow

- All traffic is collected
- Provides complete view of all network activity
- Similar to reading every word, page of a book
- Suitable for detecting large scale as well as extended, slow attacks

# Turn the Network into a Security Sensor Grid



# Packet Capturing

**Port Mirroring** – Use network switches to mirror traffic seen on ports or VLANs.

**Network Taps** - Monitor and capture packets from point-to-point links. Network taps capture and copy network packets without involving the active network components, making them suitable for most environments.

**Compliance – Forensics - Troubleshooting**

# NetFlow vs Packet Capturing



Page: 259 of 849  
Billing Cycle Dates: 09/12/11 - 10/11/11  
Account Number: 828074228  
Foundation Account Number: 08076469

## Data Detail (Continued)

479-387-2554

User Name: UNIVERSITY OF ARKANSAS FAYETTEVILLE

Rate Code: MSGU=Messaging Unlimited, IPGB=4GB Data\_Tethering

Ratio Period (PDR): AT=Anytime

Feature: SMH=SMS \$0.00, MMB=MB MMS \$0.00, MBTA=GPRS MB Dom \$10.00/1GB APN002/APN003/APN004

Item	Day	Date	Time	To/From	Type	Msg/KB/Min	Rate	Rate	Feature	In/Out	Total Charge
							Code	Pd			
54	09/12	3:56PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
55	09/12	3:56PM	479-236-9780		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
56	09/12	4:01PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
57	09/12	4:09PM	479-236-9780		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
58	09/12	4:11PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
59	09/12	4:12PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
60	09/12	4:21PM	479-236-9780		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
61	09/12	4:26PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
62	09/12	4:29PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
63	09/12	4:29PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
64	09/12	4:30PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
65	09/12	4:32PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
66	09/12	4:32PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
67	09/12	4:45PM	479-236-9780		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
68	09/12	4:51PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
69	09/12	4:56PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
70	09/12	4:57PM	479-236-9780		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
71	09/12	4:58PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
72	09/12	4:58PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
73	09/12	4:58PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
74	09/12	5:01PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	Out	0.00
75	09/12	5:01PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00
76	09/12	5:03PM	479-856-9535		MTM TEXT MESSAGE	1 Msg	MSGU	AT	SMH	In	0.00



# Routing Sinkholes

- Admins setup internal routing sinkholes to route unwanted traffic
- Many times, routing is sent to a null interface
- This is less processor intensive than blocking traffic



Same as botnet sinkhole but send other types of threats

**Sandbox:** Execute untrusted programs or code

**Honey pot:** vulnerable system designed to be a decoy and attract attackers

\*Make sure these don't become a gateway for attackers!

# Sandbox

- Environment to simulate host system
- Virtualized platform that runs various operating systems
- As malware explodes, it records behavior
- New sandboxes will run standard images from an organization
- Malware tries to detect and evade sandboxed environments



# Pre NAC

127.0.0.1



# Post NAC



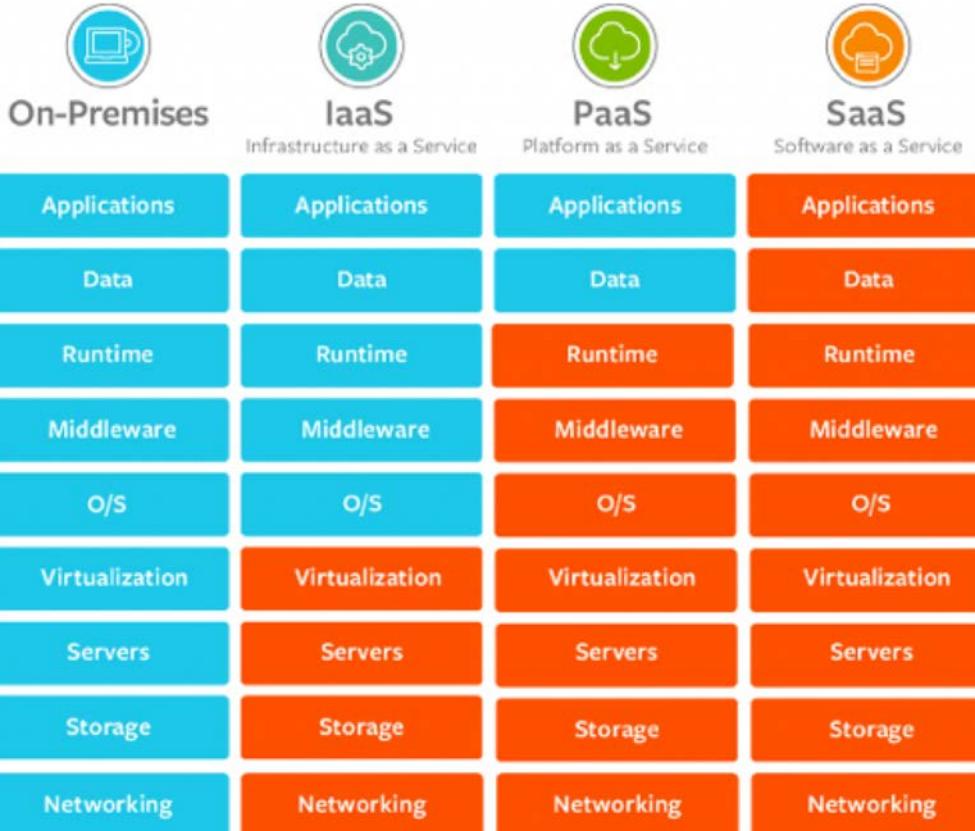
# Cloud Security



Find and contain  
problems  
fast

# Cloud Services

- SaaS – Everything in cloud via cloud service provider (CSP) responsibility (ex. DropBox)
- PaaS – Run your applications within CSP
- IaaS – Run your servers within CSP (ex. Azure, Amazon Cloud)



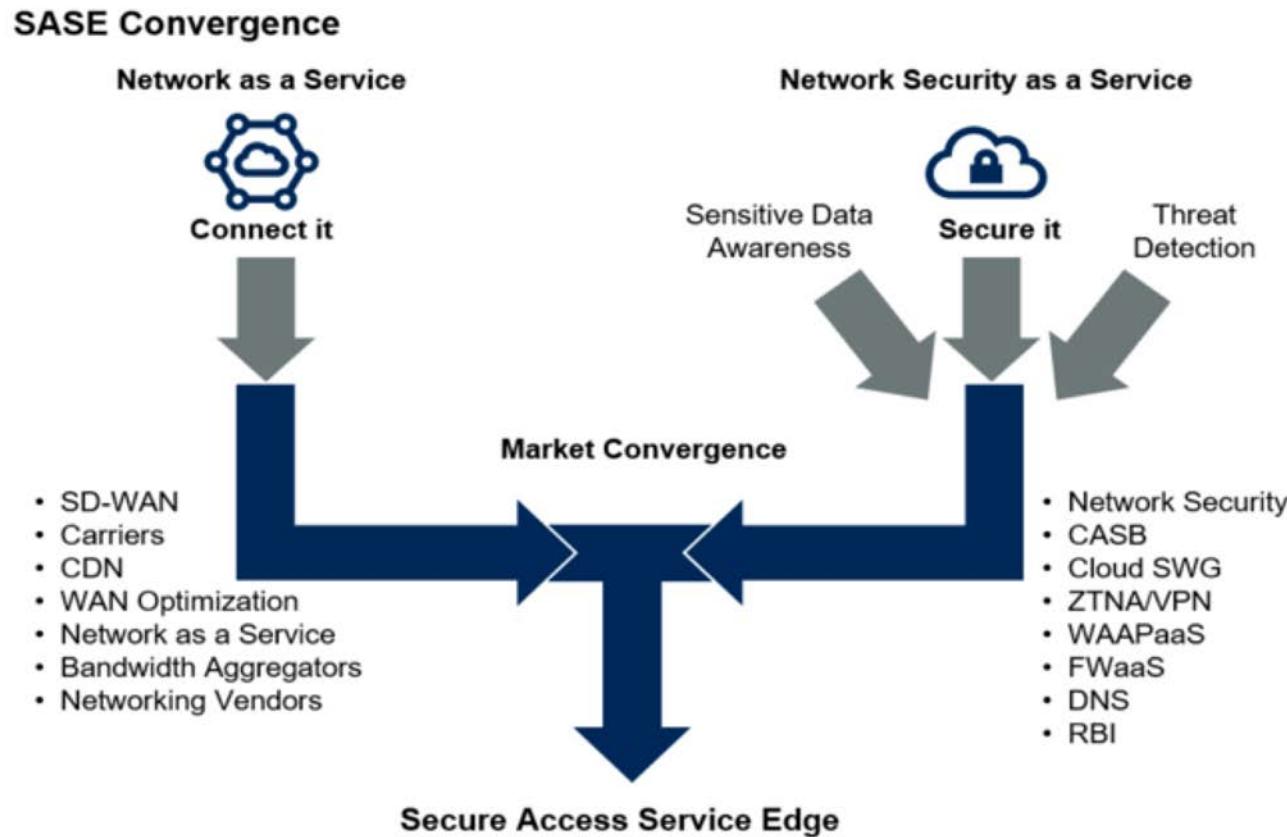
# SASE Interest Starts with Gartner Claims

*“SASE will be as **disruptive** to network and network security architectures as was architecture for datacenter design”*

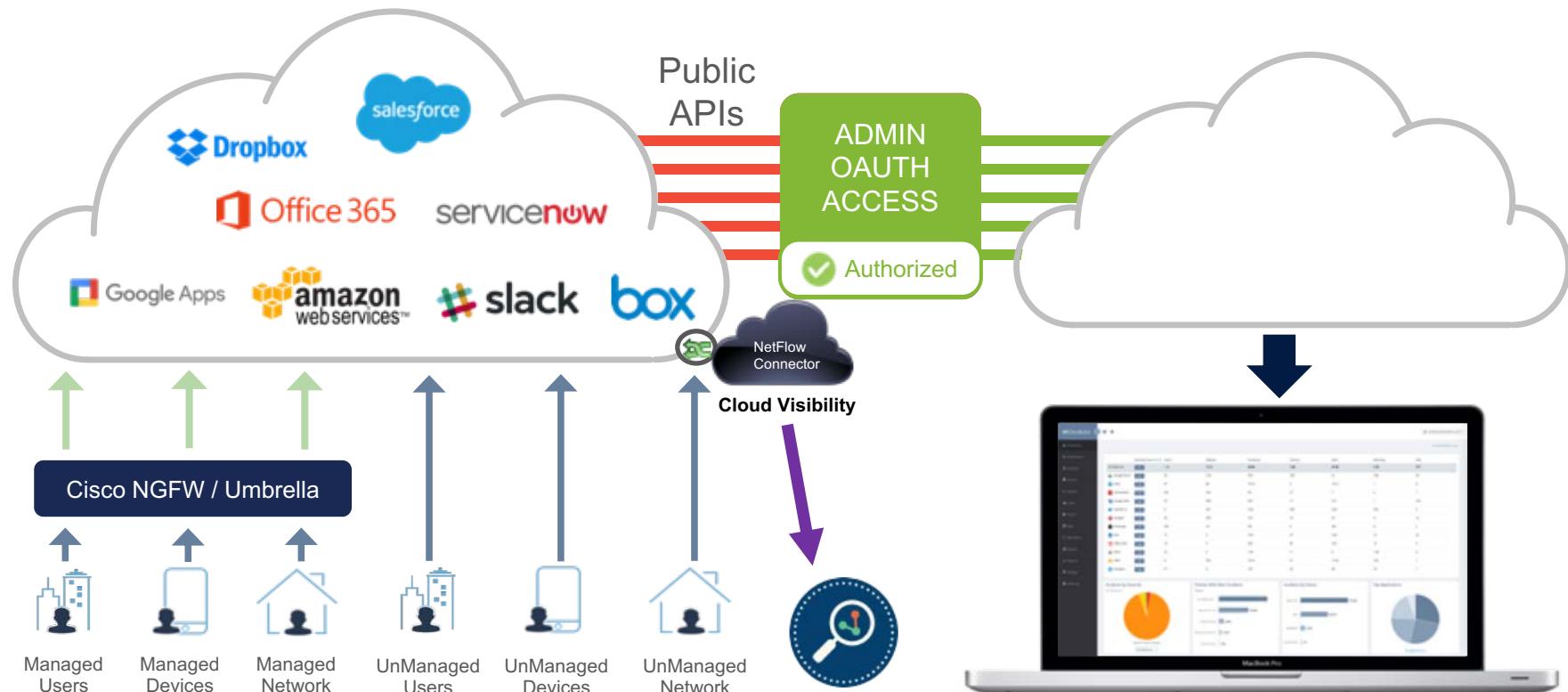
*It's a technology that Gartner has called  
**Transformational***



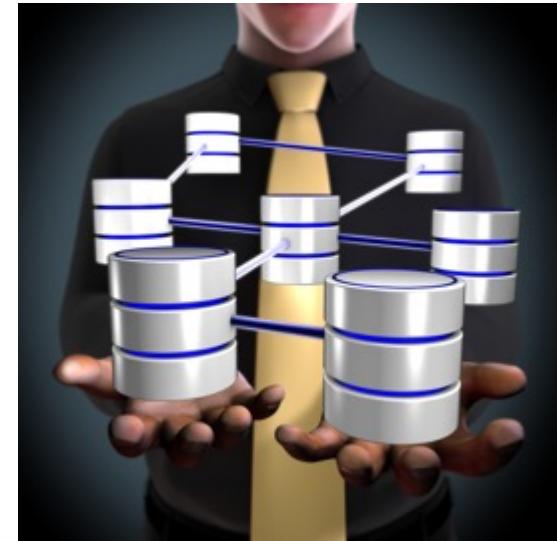
Combines **Security functions** with **WAN capabilities (SD-WAN)** to address changing enterprise traffic patterns and threats



# CASB - API Access (Cloud to Cloud)



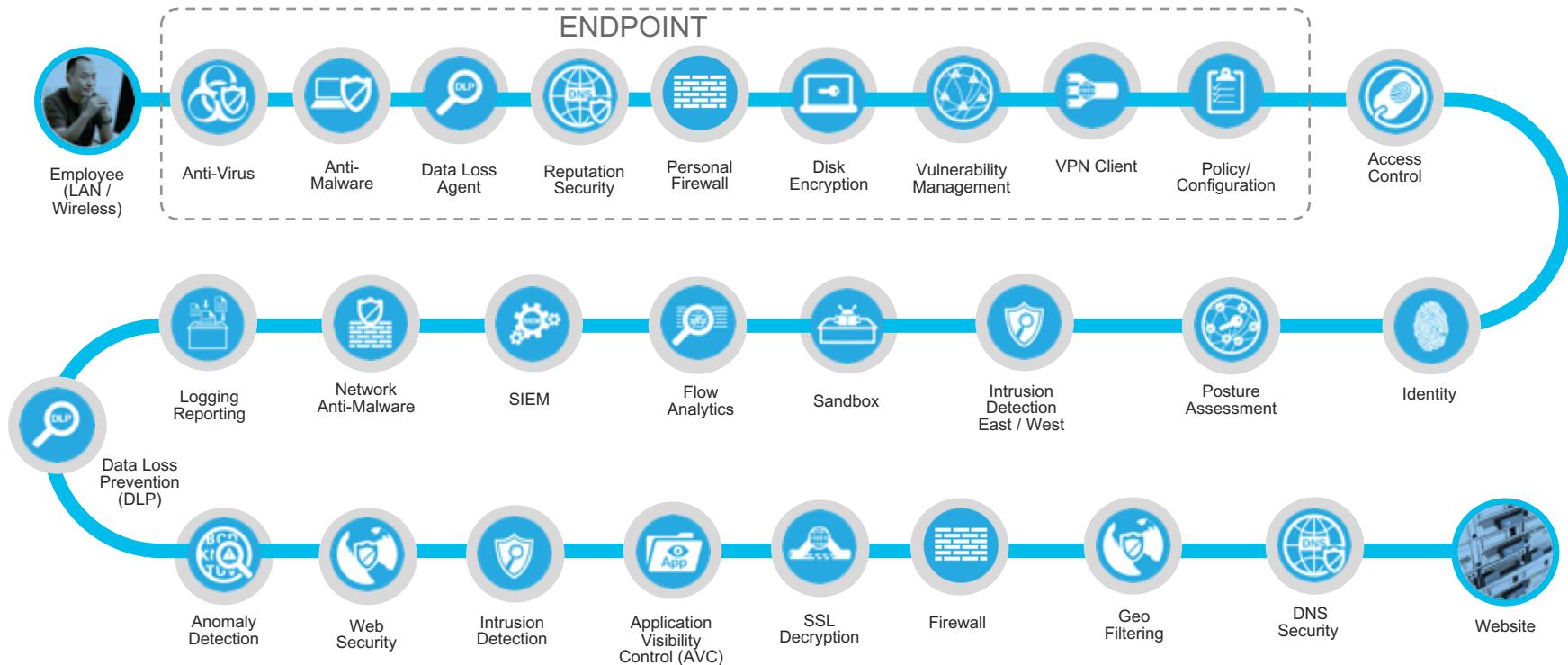
# Architecture Best Practices



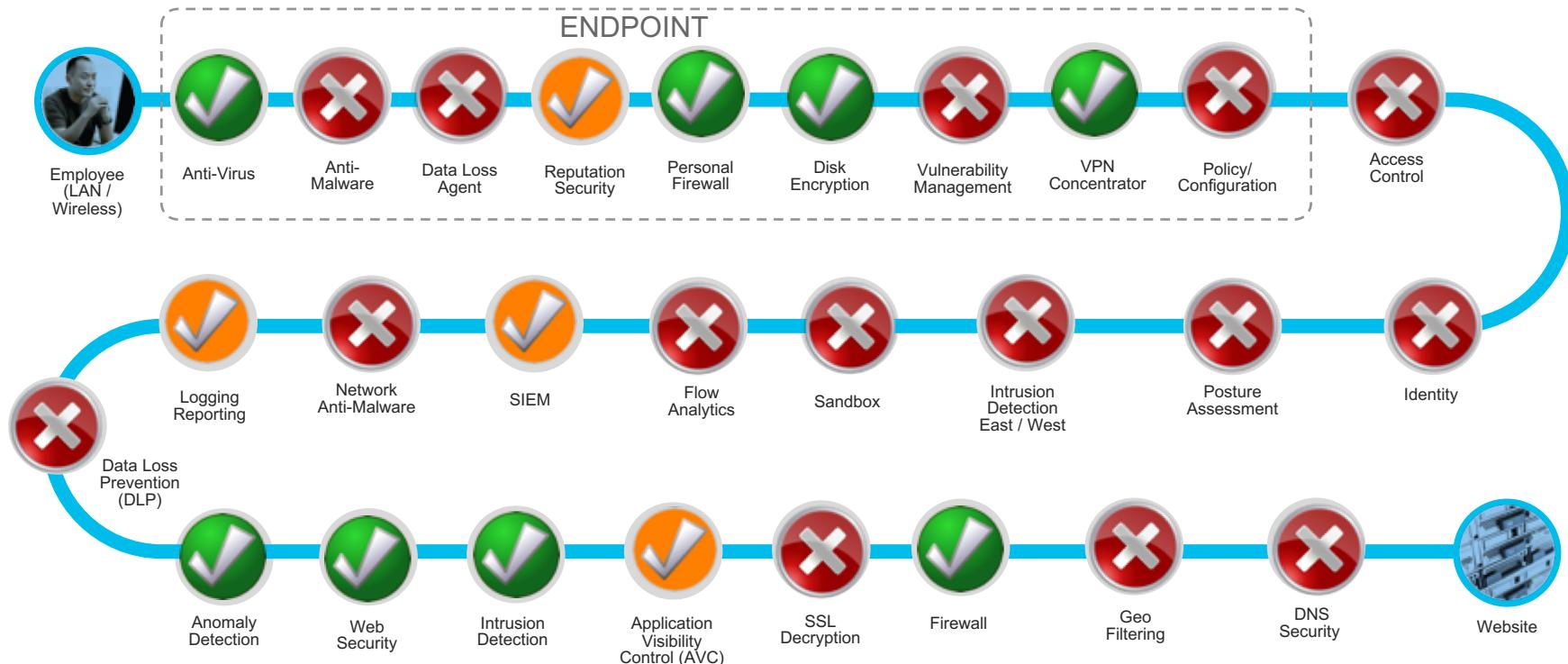
# Common Architecture Challenges

- **Single Point of Failure** - High availability / redundant systems
- **User and policy challenges**
- **Authentication and Authorization** - Multifactor authentication and account management can help
- **Data validation / Trust** – Enforcing CIA
- **Budget for improvement**
- **Install and maintenance**
- **New Complexity**
- **Lack of understanding the technology and value**

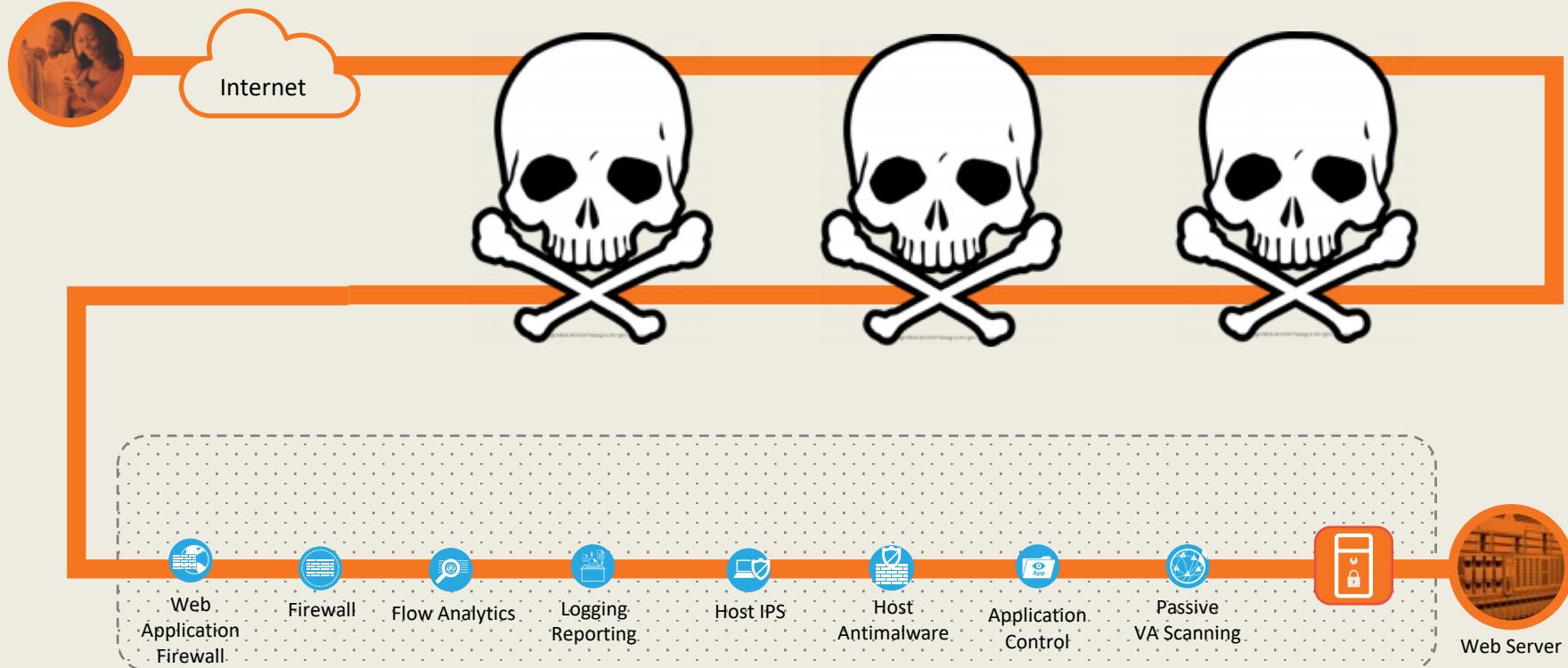
# Employee on site to Internet



# Employee on site to Internet



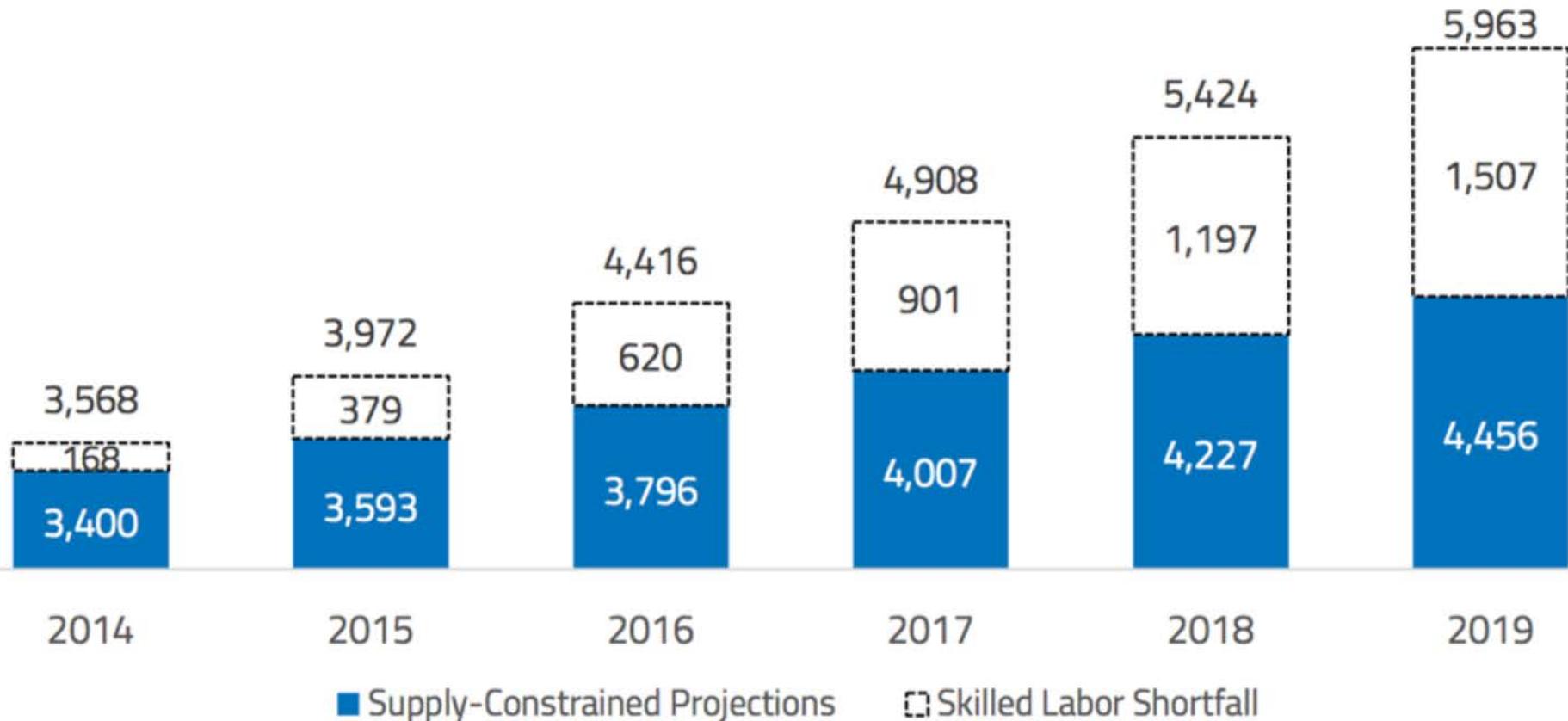
# Focusing on Datacenter



# Certification and Training



## Demand-Meeting Projections for Security Professionals (U.S. or Global)



# Which Job For You?

- **Manage Products** – Network or Security Engineer
- **Install Hardware** – Services
- **Operations** – Analyst
- **Break into things** - Pen Testing
- **Compliance** – Auditor
- **Sales** – Presales Engineer / Architect

**Specialize makes more \$\$ than generalist**

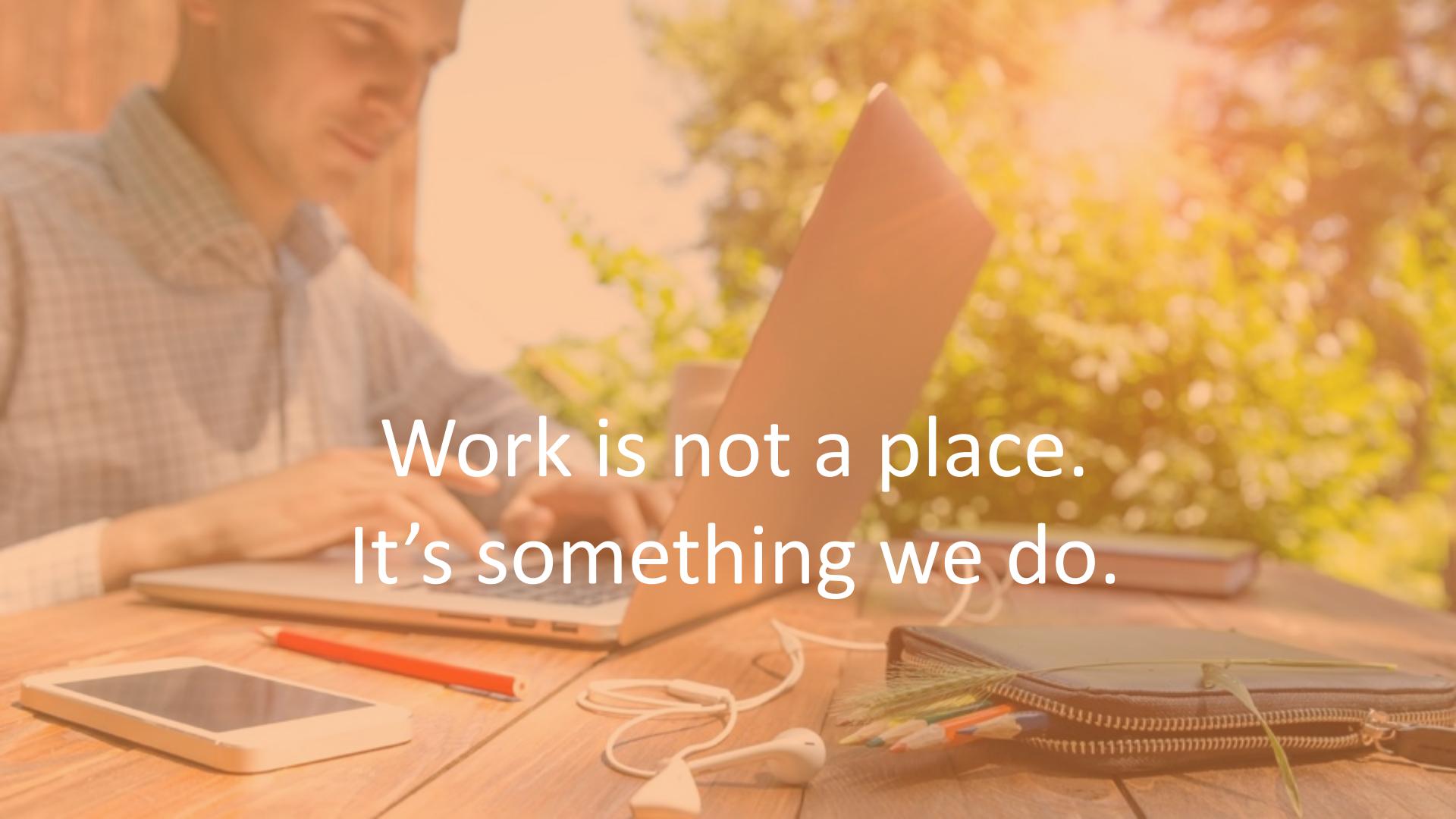
# Certifications

- CISSP – Basic Technology and Language Test
- CEH – Introduction to Pen Testing
- CHFI – Introduction to Forensics
- SANs – Many skilled exams
- OSCP (Kali) – Challenging Kali Linux Training

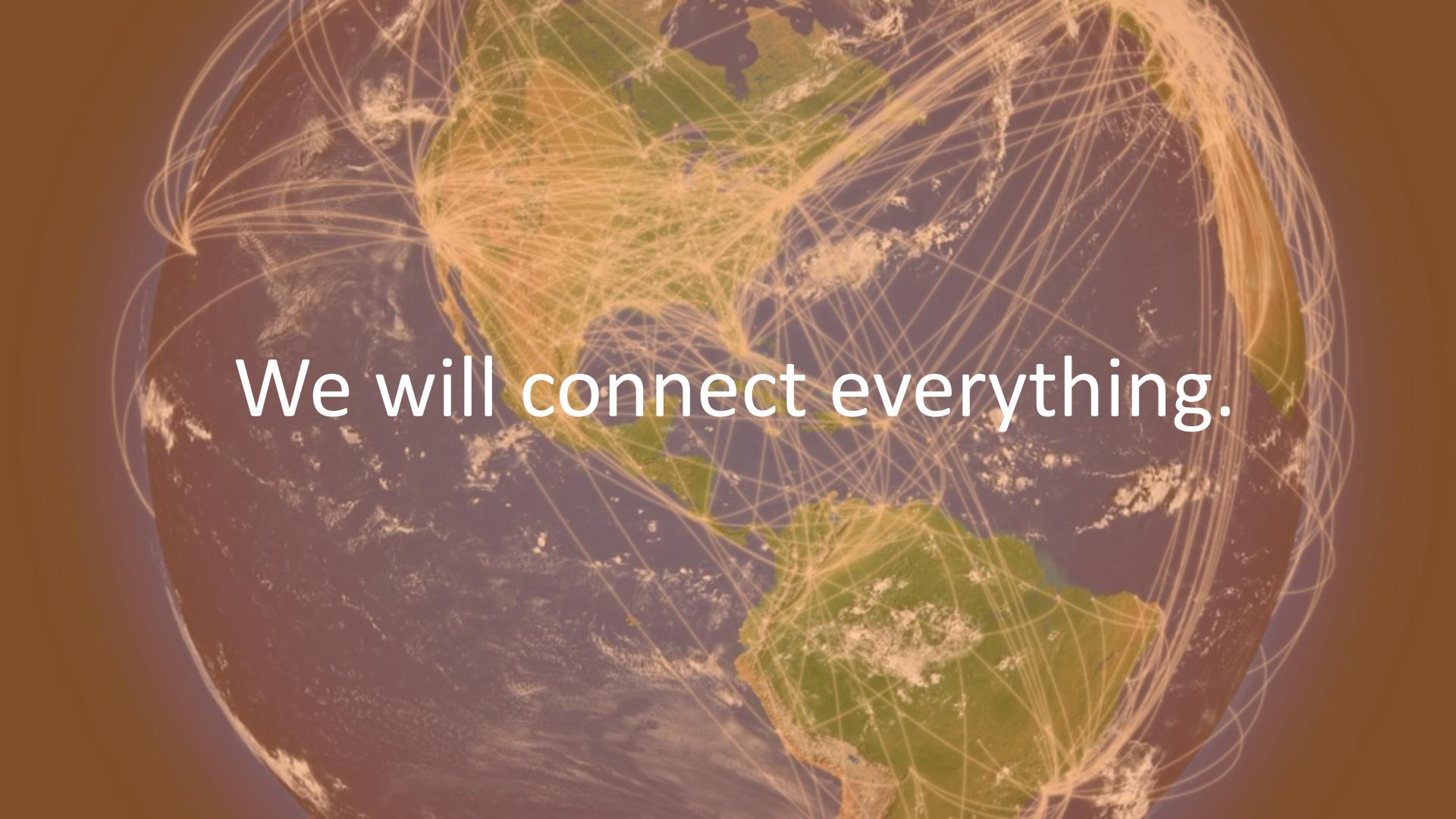
Lots of Free training too - Youtube

A black and white photograph of a man in a suit and tie, sitting at a desk in what appears to be a control room or office. He is looking towards the camera with a serious expression. In front of him is a large computer monitor displaying a map or data visualization. To his right, there are several other computer monitors and equipment. The lighting is dramatic, with strong shadows.

Are You Ready For The Next  
Threat?

A man is sitting at a wooden table outdoors, working on a silver laptop. He is wearing a grey button-down shirt. The background is filled with vibrant autumn leaves in shades of orange, yellow, and red. On the table in front of him are various items: a white smartphone, an orange pen, a pair of white headphones, a small notebook with a zipper, and several colored pencils.

Work is not a place.  
It's something we do.

A satellite photograph of the Earth showing a complex network of yellow lines crisscrossing the globe. These lines represent communication satellites and their orbital paths, creating a web-like pattern against the blue oceans and green continents.

We will connect everything.



Threats will increase.  
Volume and sophistication.

# Security is a Journey ... not a Destination!

